Цифровые технологии

КриптоАРМ Защищенная почта

Документация продукта

Релиз v6.2

Архивная документация. Актуальный релиз: v7.3

Исходная документация на CryptoARM.ru

Редакция от 26.11.2026

Правообладатель и разработчик
ООО «Цифровые технологии»

Содержание

Общие сведения

О продукте 7

Функциональность 9

Лицензирование 13

Общие вопросы 14

Криптопровайдеры 18

Установка

Установка КриптоАРМ

Установка КриптоАРМ на Windows 20

Установка КриптоАРМ на Linux 24

Установка КриптоАРМ на macOS 33

Установка КриптоПро CSP

Установка КриптоПро CSP на Windows 41

Установка КриптоПро CSP на Linux 51

Установка КриптоПро CSP на macOS 57

Проверка атрибута KeyAgreement 60

Активация лицензии

Активация лицензии КриптоАРМ 62

Активация лицензии КриптоПро CSP 65

Активация лицензии на модули TSP и OCSP 68

Начало работы

Проверка рабочего места 70

С чего начать работу с почтой 76

С чего начать работу с документами 77

Почта

Почтовые аккаунты

Управление аккаунтами

Добавление аккаунта 78

Добавление аккаунта mail.ru 82

Добавление аккаунта yandex.ru ... 85
Добавление аккаунта gmail.com ... 88
Добавление аккаунта outlook.com ... 91
Добавление аккаунта icloud.com ... 94
Добавление аккаунта rambler.ru ... 97
Действия с аккаунтами ... 100
Почтовые настройки
Настройки защищенной почты ... 104
Настройки подключения ... 109
Общие настройки ... 113
Подписи (контактная информация) ... 117
Создание и отправка писем
Создание нового письма ... 120
Отправка письма с запросом уведомлений о доставке и прочтении ... 131
Отправка письма с подписью и шифрованием ... 134
Работа с письмами
Действия с письмами ... 139
Работа с вложениями в письмах ... 150
Проверка подписи письма ... 154
Расшифрование письма ... 159
Письма с уведомлениями ... 162
Черновики писем ... 166
Удаление и восстановление письма ... 168
Организация почты
Автоматическая сортировка писем ... 172
Поиск писем ... 179
Расширенные функции
Автоматическая рассылка файлов ... 182
Работа с расширениями .eml, .p7s, .p7m ... 187
Документы
Профили подписи
Управление профилями ... 190

Описание настроек профиля ... 201

Подпись и шифрование

Подпись со стандартом CAdES ... 212

Подпись со стандартом PAdES ... 222

Подпись с созданием печатной формы ... 235

Добавление соподписи ... 248

Шифрование ... 250

Объединение подписей ... 256

Проверка и расшифрование

Проверка подписи ... 259

Снятие подписи ... 267

Расшифрование ... 270

Подпись и защита PDF

Просмотр документа ... 273

Подпись документа ... 277

Сертифицирующая подпись ... 293

Подпись с конвертацией в PDF/A ... 297

Подпись в размеченную область ... 301

Проверка подписи ... 305

Автоматизация операций

Выполнение операций в командной строке ... 309

Пример автоматизации ... 318

Управление документами

Открытие документа ... 321

Просмотр сведений ... 324

Загрузка в Архив ... 330

Прочие действия ... 333

Сертификаты

Установка личного сертификата ... 337

Установка сертификата из DSS ... 344

Создание самоподписанного сертификата ... 349

Создание запроса ... 353

Установка корневого и промежуточного сертификатов ... 360
Установка сертификатов других пользователей ... 364
Установка списка отзыва ... 368
Экспорт личного сертификата ... 370
Экспорт сертификата ... 374
Удаление сертификата ... 377
Действия с ключевыми контейнерами ... 378

Контакты

Локальные контакты

Адресные книги ... 382
Добавление контакта ... 386
Действия с контактами ... 390
Настройка аватаров ... 395
Настройка сертификатов ... 398
Группировка контактов ... 403

Внешние источники

Адресная книга LDAP ... 407
Адресная книга ALD Pro ... 413
Адресная книга CardDAV ... 419
Импорт контактов vCard ... 424

Уведомления

Центр уведомлений ... 428
Журнал событий ... 430

FAQ

Часто задаваемые вопросы ... 436
Глоссарий ... 439

API

Описание API КриптоАРМ ... 446
Команда signAndEncrypt ... 451
Команда certificates ... 469
Команда `certrequests` ... 479
Команда diagnostics ... 489

Команда startView 498
Команда mail 503

Открыть статью на сайте

О продукте

- Основные возможности
- Совместимость
- Системные требования
- Поддерживаемые операционные системы

КриптоАРМ — приложение для электронной подписи и шифрования файлов со встроенным почтовым клиентом. Приложение предназначено для обеспечения безопасного и юридически значимого обмена электронными документами с государственными структурами, коммерческими организациями и частными лицами.

Основные возможности

1. **Подпись и шифрование документов**:
    - Присоединенная и отсоединенная электронная подпись
    - Подпись со штампом времени (на подпись и данные)
    - Усовершенствованная электронная подпись
    - Проверка подписи произвольных файлов
    - Шифрование и расшифрование файлов
    - Встроенная подпись для PDF документов
2. **Защищенная электронная почта**:
    - Отправка подписанных и зашифрованных электронных писем
    - Расшифровка и проверка подписи полученных писем
    - Хранение писем в зашифрованном виде
3. **Управление контактами**:
    - Импорт контактов из каталога LDAP, ALD Pro
    - Поддержка vCard и протокола CardDAV
    - Шифрование писем и документов в адрес контактов

Совместимость

Поддерживаемые криптопровайдеры

- КриптоПро CSP (версия 5.0 и выше)
- OpenSSL (версия 1.1.1, без поддержки ГОСТ-алгоритмов)

Поддерживаемые ключевые носители

- Рутокен
- JaCarta
- Esmart

Полный список поддерживаемых ключевых носителей можно найти в формуляре криптопровайдера КриптоПро CSP. Информацию о поддерживаемых носителях можно найти на сайте cryptopro.ru.

Системные требования

Компонент	Минимальная конфигурация	Рекомендуемая конфигурация
Процессор	x86-64, 1.0 ГГц	x86-64, 2.0 ГГц+
ОЗУ	2 ГБ	4 ГБ+
Дисковое пространство	500 МБ	5 ГБ+
Дисплей	1024×768	1920×1080+

Поддерживаемые операционные системы

Клиентские:

- Microsoft Windows 8.1, 10, 11
- Ubuntu 20.04, 22.04
- macOS 11 Big Sur, 12 Monterey, 13 Ventura, 14 Sonoma, 15 Sequoia
- Astra Linux Special Edition 1.7 Смоленск
- Альт Рабочая станция 10, К 10, 11, К 11
- Альт 10 Образование
- РЕД ОС 7.3
- РОСА ХРОМ 12 Рабочая станция
- Атлант, релиз – Alcyone

Серверные:

- Windows Server 2016
- Windows Server 2019
- Ubuntu Server 20.04, 22.04
- CentOS 8
- Альт Сервер 10
- РЕД ОС Сервер 7.3
- РОСА ХРОМ 12 Сервер

Открыть статью на сайте

Функциональность

Возможности	
Работа с документами	работа с результатами выполнения операций с документами
	хранение копии документов, полученных в результате выполнения операций
	переход в мастер «Подпись и шифрование», «Проверка и расшифрование», «Подпись и защита PDF»
	работа с почтовыми вложениями: открыть, добавить в мастер, отправить, показать в папке
Электронная подпись	электронная подпись и проверка подписи произвольных файлов на поддерживаемых платформах; размер файла не может быть больше, чем свободная оперативная память, гарантированный размер файла — 2 Гб
	добавление электронной подписи (функция создания соподписи) на поддерживаемых платформах; размер файла не может быть больше, чем свободная оперативная память, гарантированный размер файла — 2 Гб
	создание присоединенной и отсоединенной электронной подписи
	создание подписи стандарта CAdES-BES, CAdES-T, CAdES-X Long Type 1, CAdES-A
	подпись сертификатом DSS
	формирование отчёта о проверке электронной подписи документа в формате .pdf
	снятие электронной подписи с документа
	объединение электронных подписей
Подпись PDF	подпись и сертификация файлов в формате PDF
	создание подписи стандарта PAdES-BES, PAdES-T, PAdES-X Long Type 1, PAdES-A
	хранение копии документов, полученных в результате операций

Возможности	
	разметка областей под подписи и подписантов
	добавление произвольной области под изображение или текст
	конвертация в формат PDF/A-2b и PDF/A-3b
Шифрование/расшифрование	шифрование и расшифрование файлов на поддерживаемых платформах; размер файла не может быть больше, чем свободная оперативная память, гарантированный размер файла — 2 Гб
	удаление исходных файлов после шифрования
	шифрование по стандарту PKCS#7
	шифрование в адрес нескольких получателей
	шифрование в адрес контактов
	расшифрование сертификатом DSS
Архивирование	архивирование файлов перед шифрованием; размер файла не может быть больше, чем свободная оперативная память, гарантированный размер файла — 2 Гб
	разархивирование из формата .zip
Управление контактами	создание, редактирование, удаление и восстановление локальных контактов
	поиск, группировка, сортировка контактов
	управление колонками в списке контактов
	добавление сертификата к контакту
	импорт контактов из каталога LDAP
	поддержка адресной книги ALD Pro
	поддержка vCard
	поддержка протокола CardDAV
	уровни вложенности групп контактов в виде древа
	поиск дубликатов и объединение контактов в одну запись
	шифрование документов в адрес контактов
	отправка писем в адрес группы

Возможности	
Управление сертификатами и ключами	отображение сертификатов и привязанных к ним закрытых ключей относительно хранилищ для поддерживаемых криптопровайдеров
	проверка корректности выбранного сертификата с построением цепочки доверия и скачиванием актуального списка отзыва
	просмотр свойств сертификата электронной подписи
	хранение закрытых ключей на носителях Рутокен (Актив), JaCarta (Аладдин Р.Д.), ESMART (ISBC) при условии использования криптопровайдера КриптоПро CSP
	создание запросов на сертификат
	импорт сертификатов с привязкой к закрытому ключу
	экспорт сертификатов
	удаление сертификатов
	импорт сертификатов из DSS
	формирование отчёта действительности сертификата электронной подписи
Почта	добавление почтового аккаунта для подключения к почтовому серверу по протоколам SMTP, SMTPS, IMAP, IMAPS, POP3
	добавление почтового аккаунта Microsoft Exchange, Communigate
	редактирование настроек почтового аккаунта
	удаление подключённого аккаунта
	добавление нескольких почтовых аккаунтов
	работа с письмами — получение, просмотр, отправка, хранение, удаление (в том числе с почтового сервера), добавление вложений, отправка файлов с устройства в виде рассылки; синхронизация писем с почтовым сервером
	уведомления о получении/прочтении писем
	поиск и фильтрация писем

Возможности	
	сортировка списка писем
	группировка и отображение писем в цепочки
	перенос писем между папками активного аккаунта
	подпись и шифрование электронных писем с поддержкой российских криптоалгоритмов; автоматическая расшифровка и проверка подписи для полученных писем
	просмотр свойств электронной подписи письма
	формирование отчёта о проверке электронной подписи письма в формате .pdf
	хранение писем в зашифрованном виде
	хранение писем локально на устройстве
Работа с журналом событий и уведомлениями	отображение списка событий по уровням детализации
	просмотр уведомлений о событиях
	сохранение в формате .log
	отправка в формате .log
	распечатка информации о событиях
	загрузка архива
	отображение в папке

Открыть статью на сайте

Лицензирование

- Общая информация о лицензиях
- Пробная лицензия

Общая информация о лицензиях

Для выполнения криптографических операций с алгоритмами ГОСТ требуется действующая лицензия «КриптоАРМ версии Про». Доступны следующие варианты лицензии:

- **Пробная лицензия** (30 дней)
- **Годовая лицензия**
- **Бессрочная лицензия**

Приобрести лицензии можно в официальном интернет-магазине cryptoarm.ru.

Пробная лицензия

Активация пробного периода

При первом запуске КриптоАРМ автоматически активируется 30-дневная пробная лицензия, которая позволяет ознакомиться со всеми функциями продукта и протестировать работу криптографических операций с алгоритмами ГОСТ.

Продление пробного периода

Если для знакомства со всеми возможностями КриптоАРМ недостаточно ознакомительного периода, вы можете получить дополнительную лицензию, написав в техническую поддержку support@trusted.ru.

Открыть статью на сайте

Общие вопросы

- Изменение раздела при запуске
- Выставление оценки
- Изменение оценки
- Определение установленной версии КриптоАРМ
- Поиск документации

Изменение раздела при запуске

Способ 1:

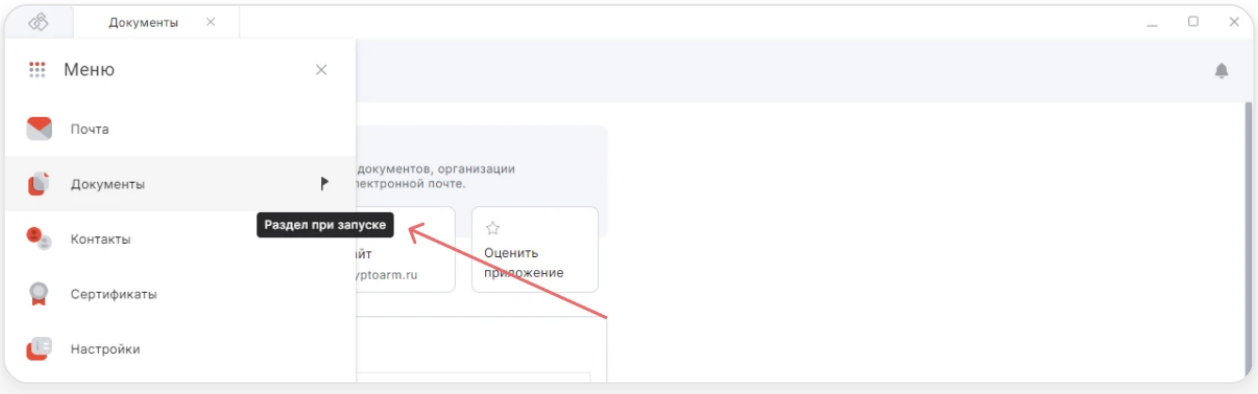
1. Откройте раздел **Настройки**.
2. Выберите необходимый раздел в блоке **Интерфейс**.

Выбранный раздел откроется автоматически при следующем запуске приложения.

Способ 2:

1. Откройте меню с разделами приложения по кнопке **Меню**, которая расположена в верхнем левом углу окна.
2. Наведите курсор мыши на раздел, который должен открываться при запуске приложения.
3. Нажмите на кнопку **Показывать при запуске**.

Выбранный раздел откроется автоматически при следующем запуске приложения.



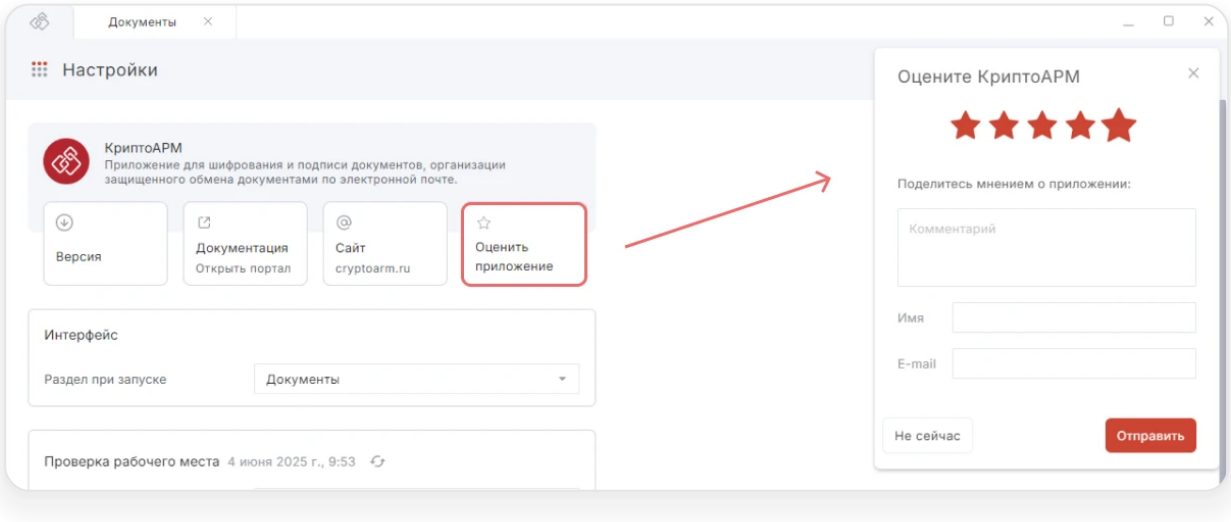
Выставление оценки

Вы можете оценить приложение и поделиться мнением.

1. Откройте раздел **Настройки**.

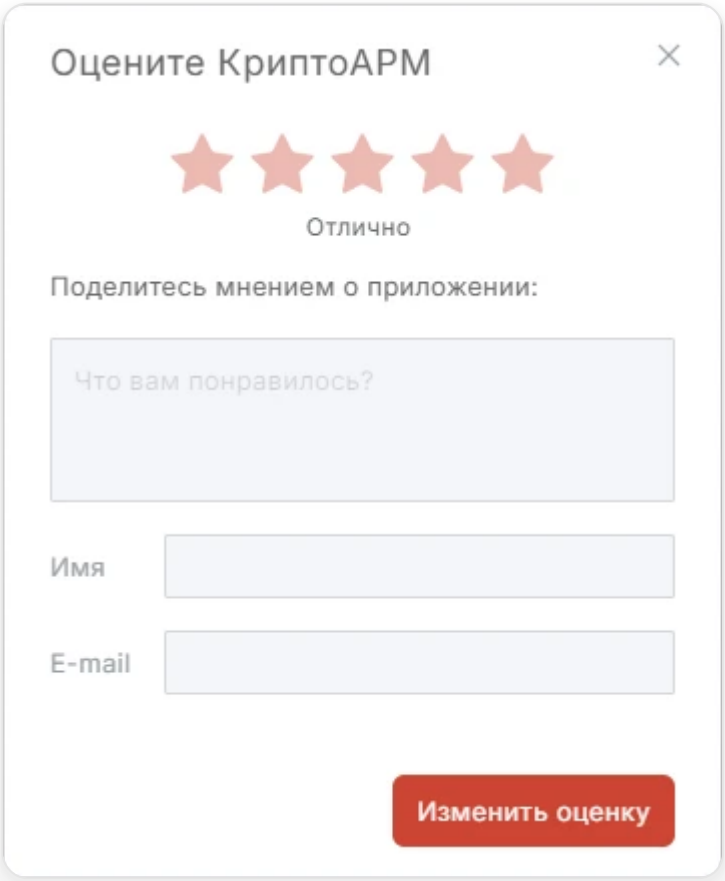
2. Нажмите на **Оценить приложение** в блоке со сведениями о продукте.
3. Откроется окно **Оцените КриптоАРМ**:
    - Поставьте оценку,
    - Оставьте свой отзыв.
    - Укажите имя и адрес электронной почты.

    Поля с отзывом, именем и адресом почты можно оставить пустыми.
4. Нажмите **Отправить** для отправки отзыва.



Изменение оценки

1. Откройте раздел **Настройки**.
2. Нажмите на **Оценить приложение** в блоке со сведениями о продукте..
3. Откроется окно **Оцените КриптоАРМ**.
4. Нажмите **Изменить оценку**.



5. Внесите изменения.
6. Нажмите **Отправить** для отправки отзыва.

Определение установленной версии КриптоАРМ

Чтобы узнать, какая версия КриптоАРМ установлена на вашем компьютере, перейдите в раздел **Настройки**. Номер версии будет указан в первом блоке со сведениями о продукте.

Поиск документации

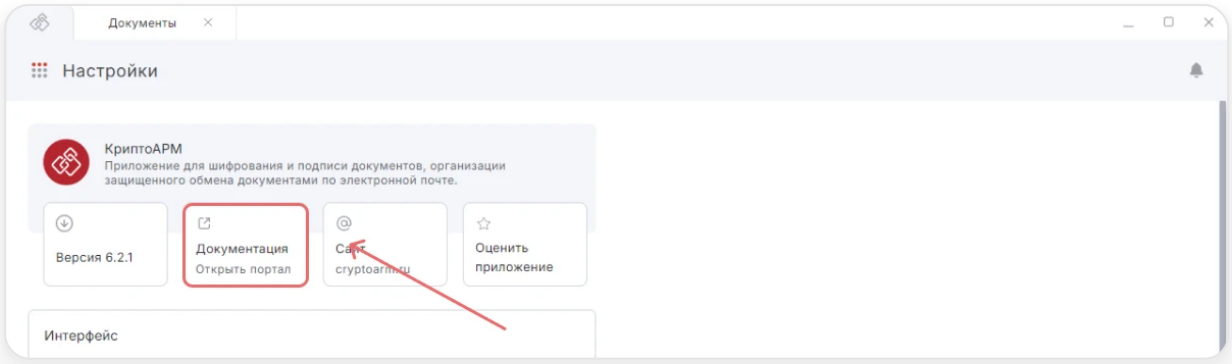
Руководство пользователя, ответы на часто задаваемые вопросы и описание API КриптоАРМ размещены на портале документации на сайте cryptoarm.ru.

Перейти на портал документации можно из приложения.

Чтобы открыть портал документации:

1. Откройте раздел **Настройки**.
2. Нажмите на виджет **Документация** в блоке со сведениями о продукте.

3. Ссылка на портал будет открыта в браузере по умолчанию.



Открыть статью на сайте

Криптопровайдеры

- Основные понятия
- Особенности в российском сегменте

Основные понятия

Что такое криптопровайдер

Криптопровайдер (CSP - Cryptography Service Provider) - это программный модуль, интегрируемый в операционную систему для выполнения криптографических операций. Он выполняет ключевые функции:

- Управление криптографическими ключами
- Генерация и проверка электронных подписей
- Шифрование и расшифрование данных
- Обеспечение целостности информации

Принцип работы

Криптопровайдер действует как посредник между:

1. Операционной системой
2. Пользовательскими приложениями
3. Аппаратными средствами (токенами, смарт-картами)

Особенности в российском сегменте

В России нельзя использовать встроенные CSP Windows, поскольку продукты Microsoft не сертифицированы в нашей стране. Это означает, что они не подходят для работы с государственными органами. Поэтому в России применяются программы от других криптосервисов.

Для работы с алгоритмами ГОСТ в КриптоАРМ нужен криптопровайдер КриптоПро CSP от компании «КриптоПро».

Криптопровайдер СКЗИ КриптоПро CSP — специальная программа, осуществляющая криптографические операции на устройстве:

- Поддерживает российские стандарты ГОСТ
- Имеет необходимые сертификаты
- Обеспечивает юридическую значимость электронной подписи

> ⚠️ **Примечание**: Без лицензии на данный криптопровайдер нельзя подписывать электронные письма и документы.

Инструкции по установке

Выберите вашу операционную систему:

- Windows
- macOS
- Linux

Открыть статью на сайте

Установка КриптоАРМ на Windows

- Подготовка к установке
- Установка

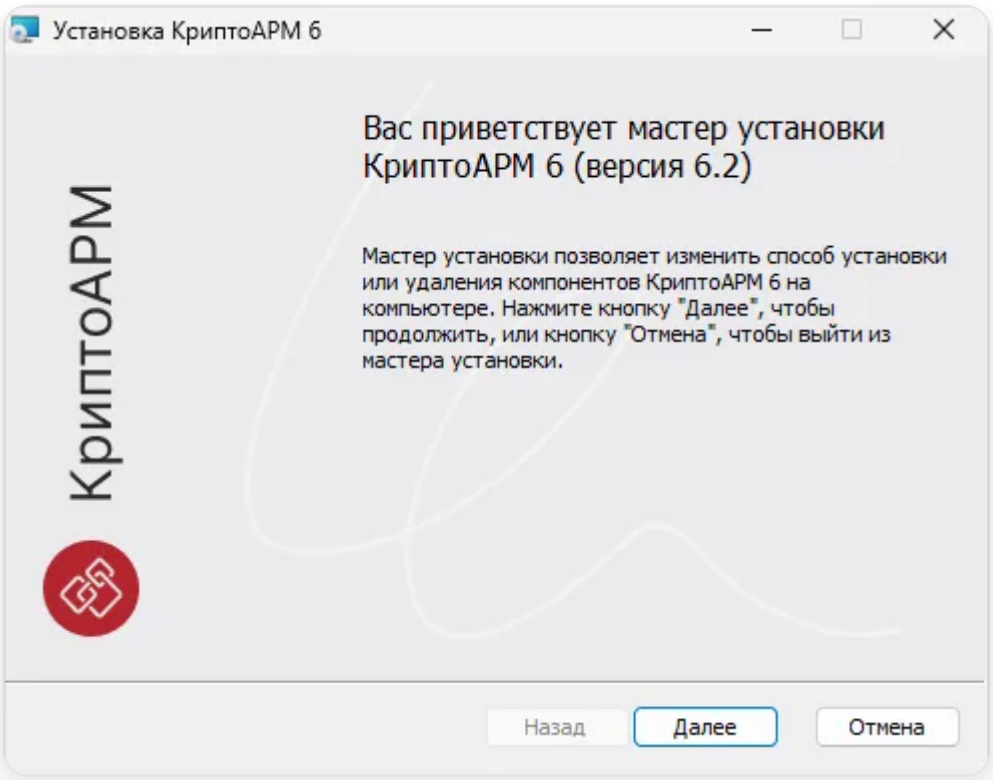
Подготовка к установке

1. Скачайте установочный файл из официальных источников:
    - Официальный сайт КриптоАРМ
    - Сайт компании-разработчика Trusted.ru
2. При необходимости установите пакеты Visual Studio C++:
    - VS C++ 2013 (x64),
    - VS C++ 2019 (x64).

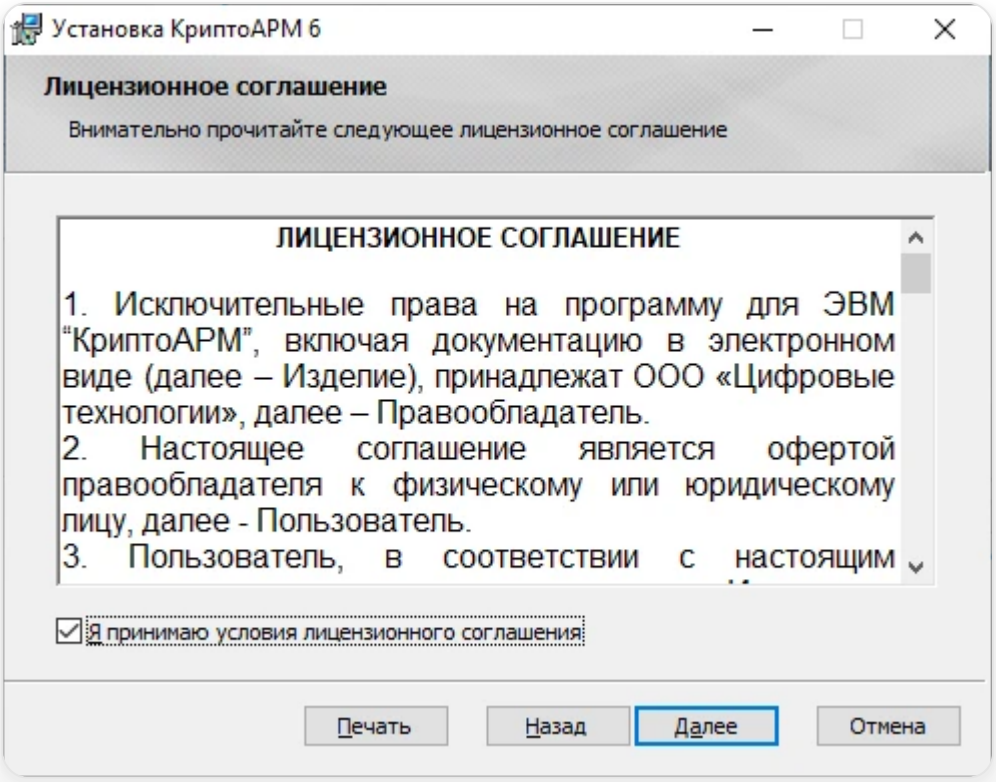
Установка

> ⚠️ **Примечание**: Для установки приложения требуются права администратора.

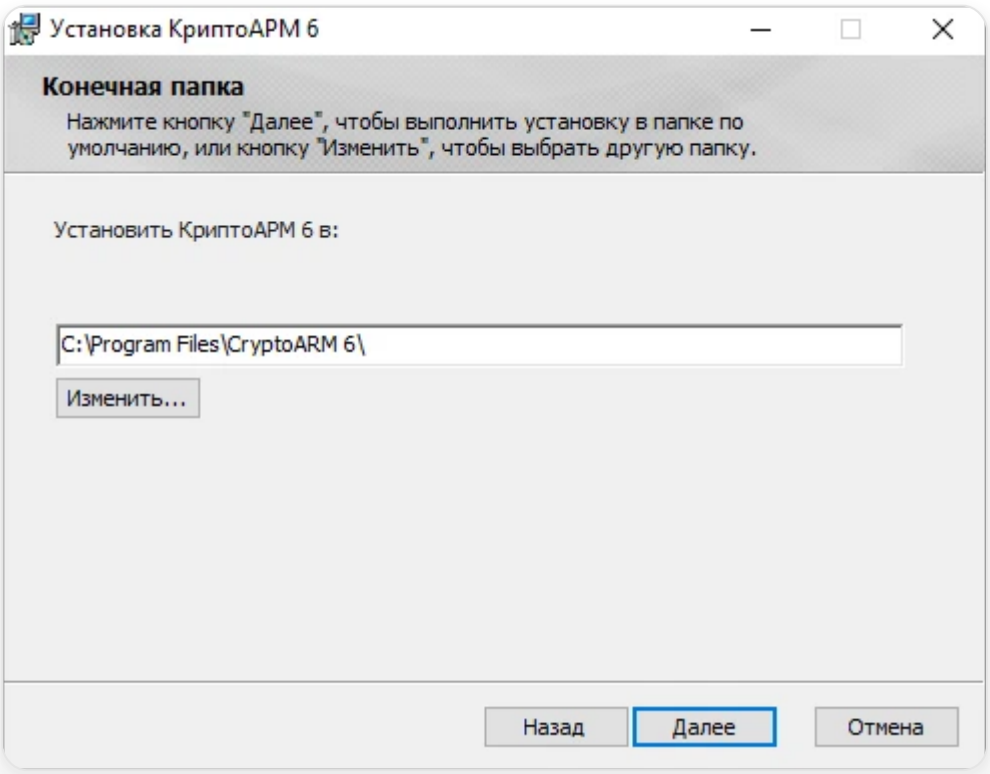
1. Запустите установочный файл.
2. Откроется мастер установки. Нажмите **Далее**.



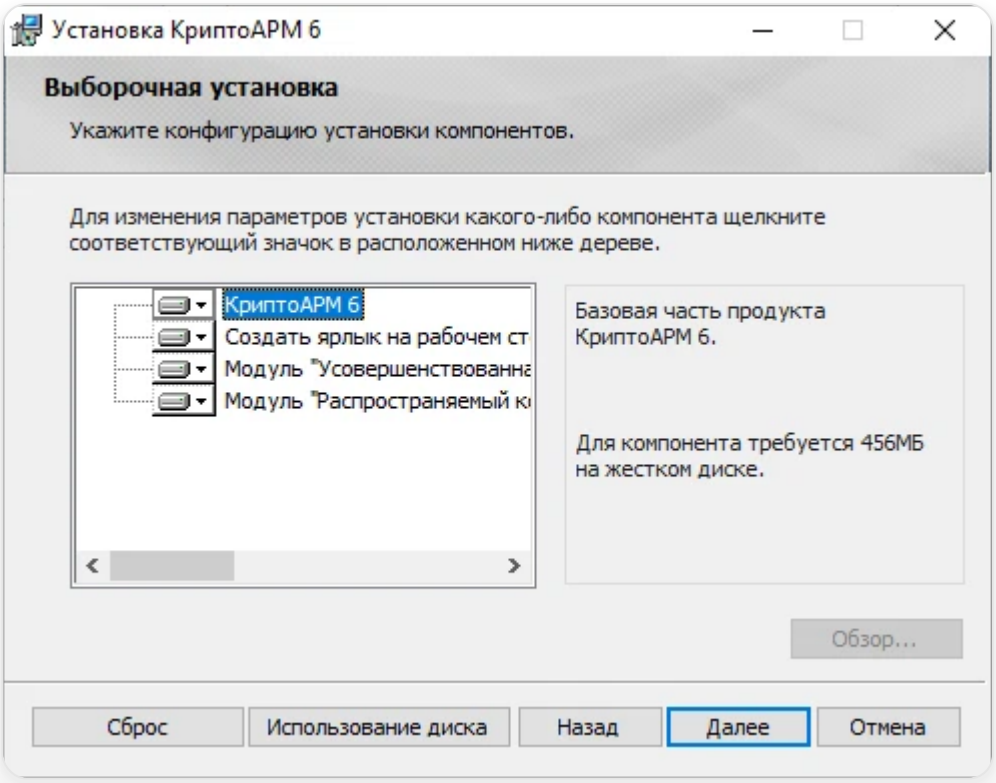
3. Ознакомьтесь с условиями лицензионного соглашения. Если вы согласны со всеми пунктами, нажмите **Принять**. Затем нажмите **Далее**.



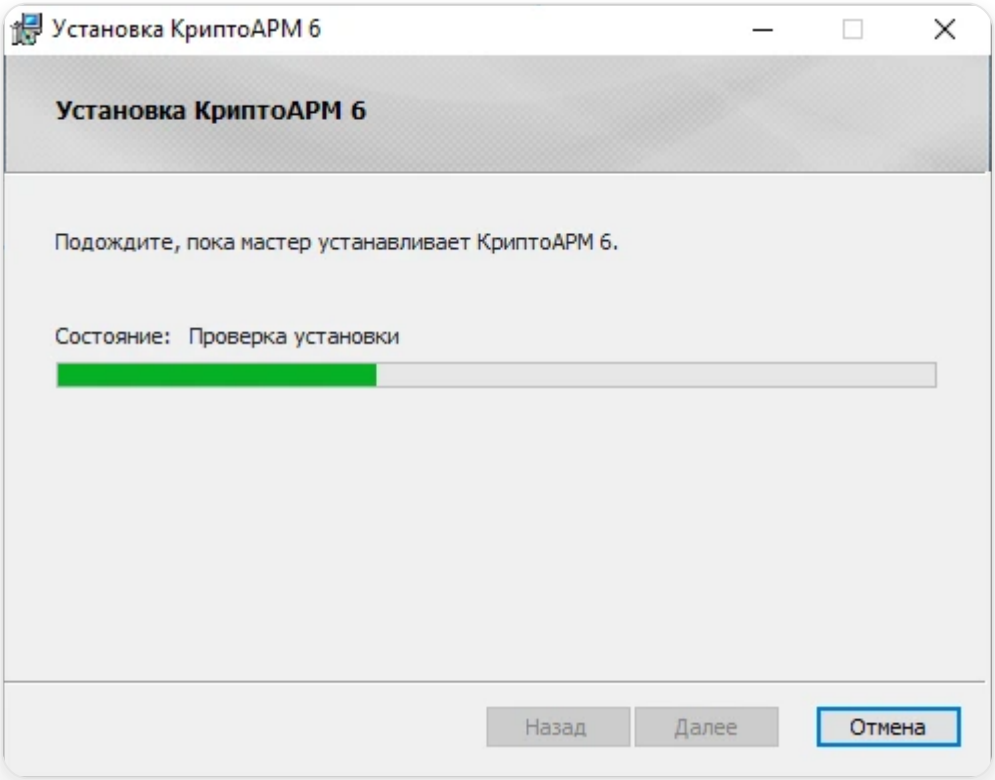
4. Выберите каталог для установки приложения. По умолчанию приложение устанавливается в каталог `C:\Program Files\CryptoARM 6\`.



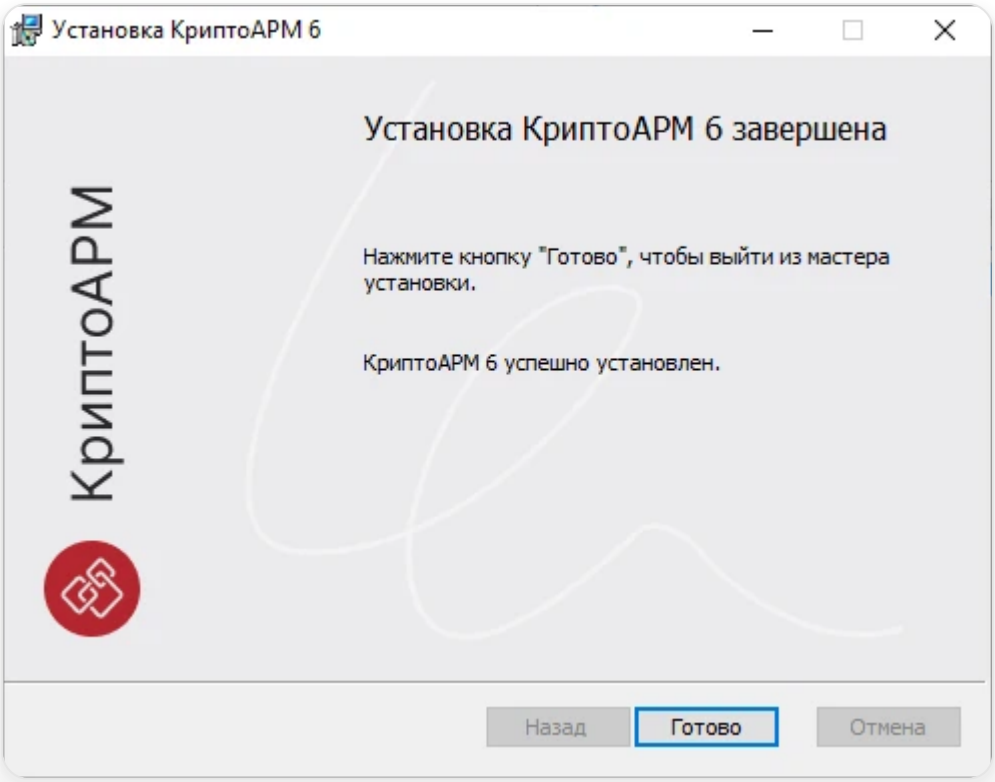
5. При необходимости отключите создание ярлыка на рабочем столе и установку модулей для создания усовершенствованной подписи.



6. Нажмите **Установить**.



Для закрытия мастера нажмите кнопки **Готово**.



Программа успешно установлена.

Открыть статью на сайте

Установка КриптоАРМ на Linux

- Подготовка к установке
- Установка RPM-пакета
- Установка DEB-пакета
- Удаление КриптоАРМ

Подготовка к установке

1. Скачайте пакет установки **КриптоАРМ** в формате `.rpm` или `.deb` из официальных источников:
    - Официальный сайт КриптоАРМ
    - Сайт компании-разработчика Trusted.ru
2. Убедитесь, что у вас есть права суперпользователя (`root`) или возможность использовать `sudo`.

> ⚠️ **Примечание**: Для Ubuntu версии 20.04 требуется дополнительная установка:
>
> - `sudo apt install libtidy-dev`
> - `sudo apt install libctemplate-dev`

Установка RPM-пакета

Через терминал

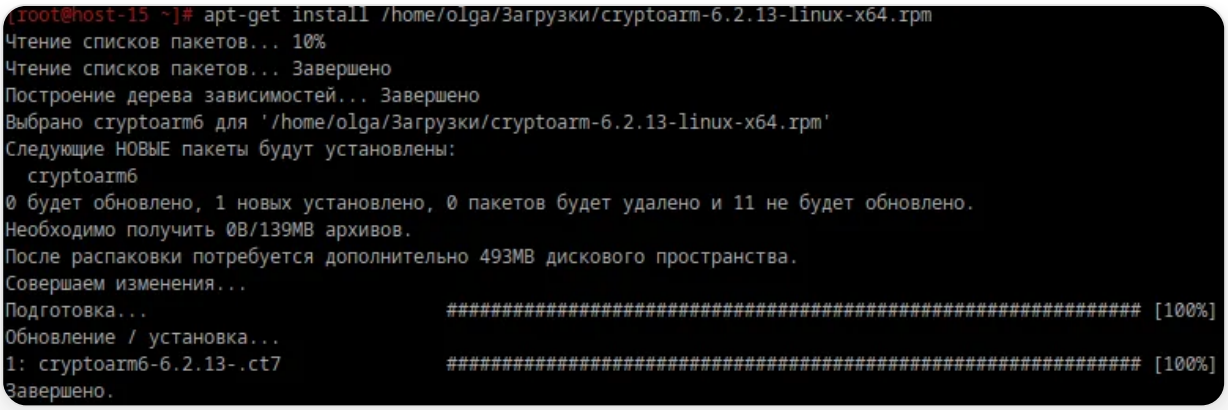
1. Откройте терминал.
2. Выполните команду для установки пакета:
    - Если вы находитесь в той же папке, что и пакет:

```
apt-get install имя_пакета.rpm # ALT Linux, Astra Linux CE, RedOS
dnf install имя_пакета.rpm     # ROSA
```

    - Если пакет находится в другой папке:

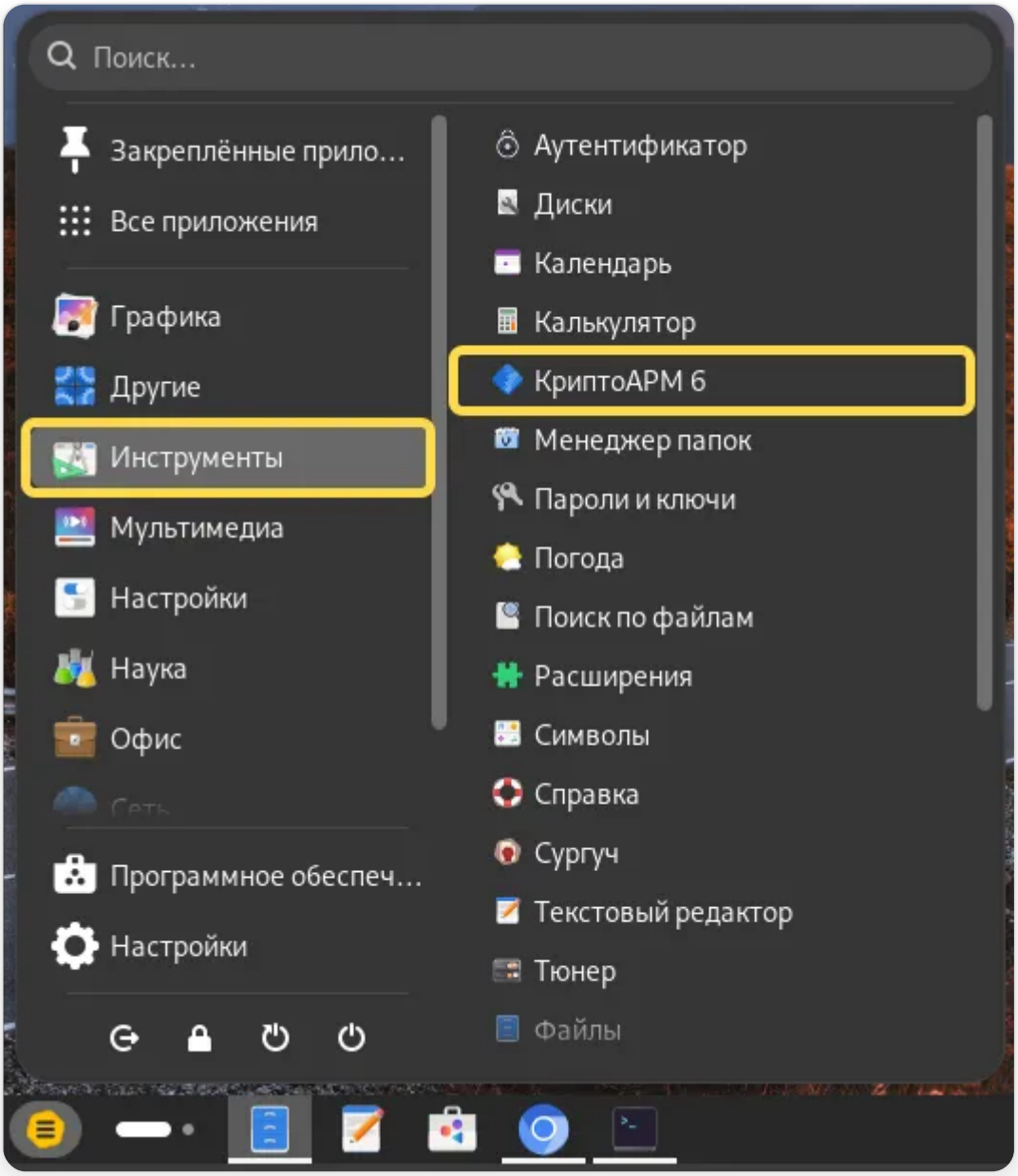
```
apt-get install /{путь_до_файла}/имя_пакета.rpm
```

3. Дождитесь окончания установки.



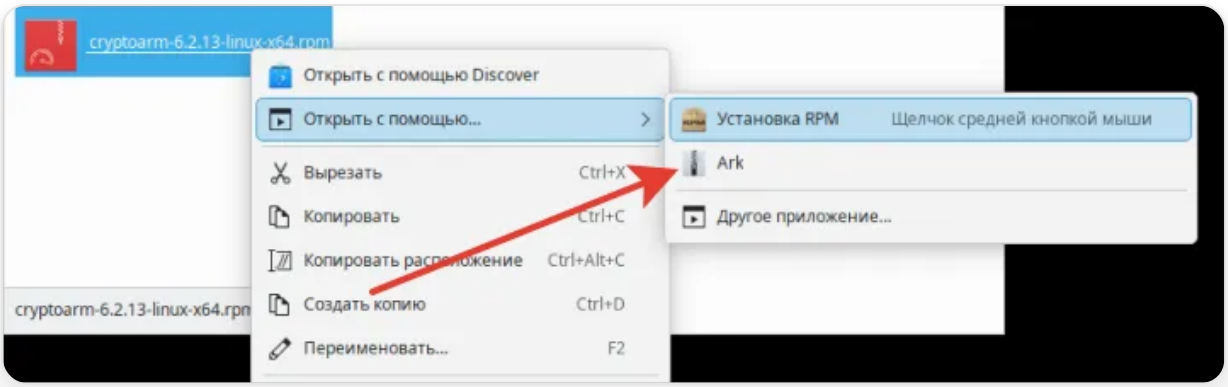
> 📌 По умолчанию приложение устанавливается в каталог `/opt/cryptoarm_6/`.

После установки приложение автоматически появляется в меню системы. Например, в **Альт Рабочая станция 11.1** приложение можно найти в разделе **Инструменты**.

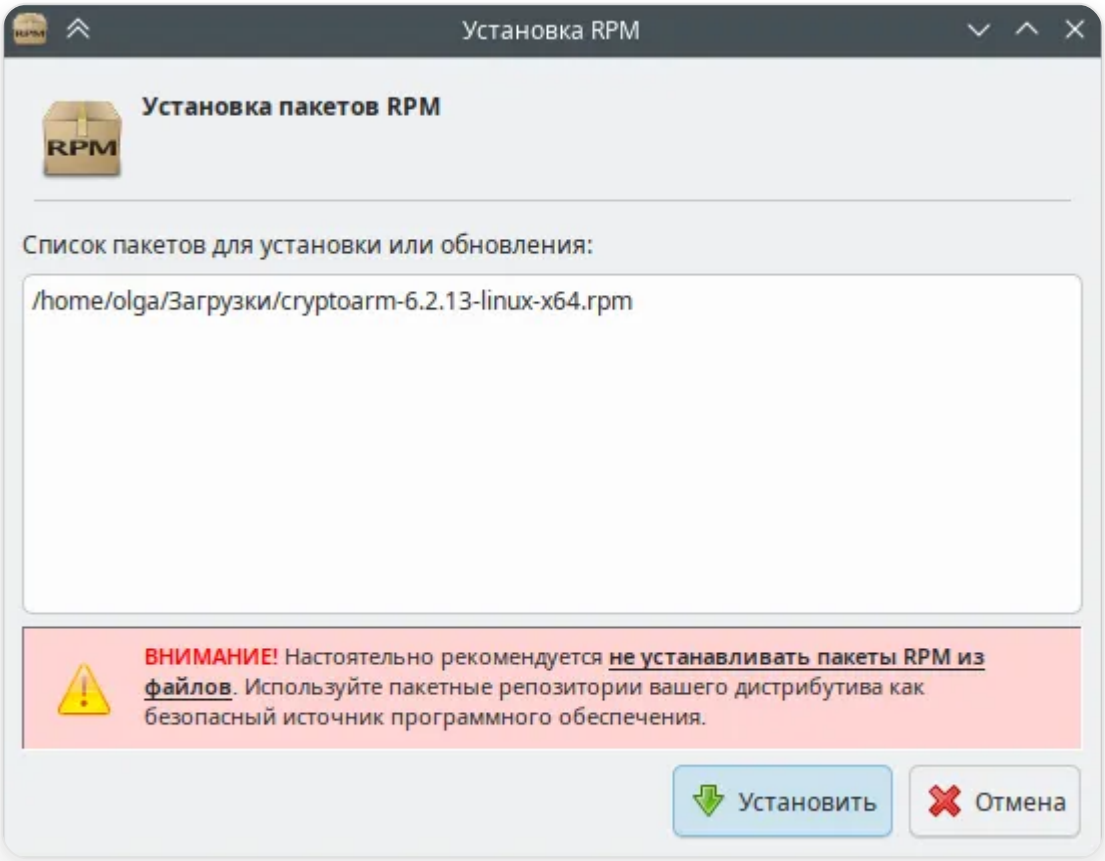


Через графический интерфейс

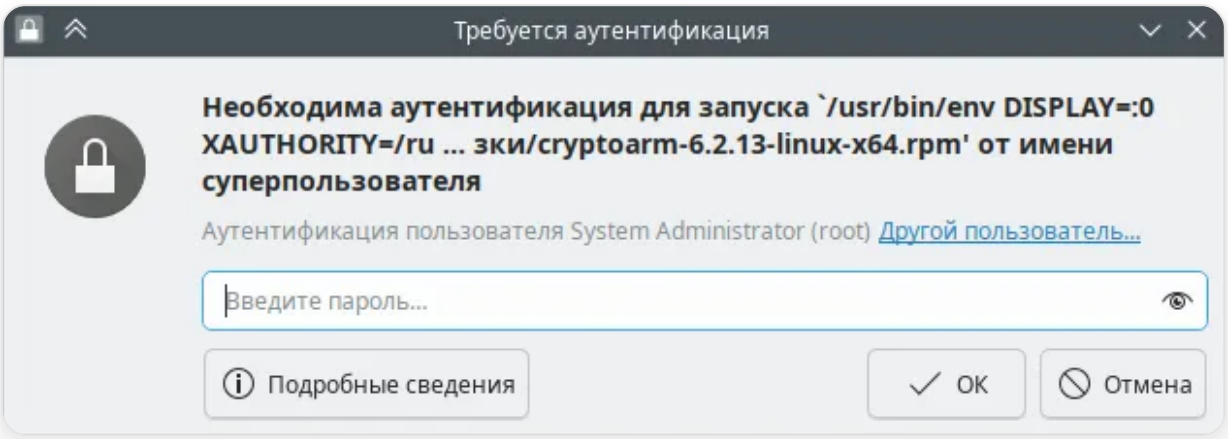
1. Откройте установочный файл `.rpm` через установщик пакетов.



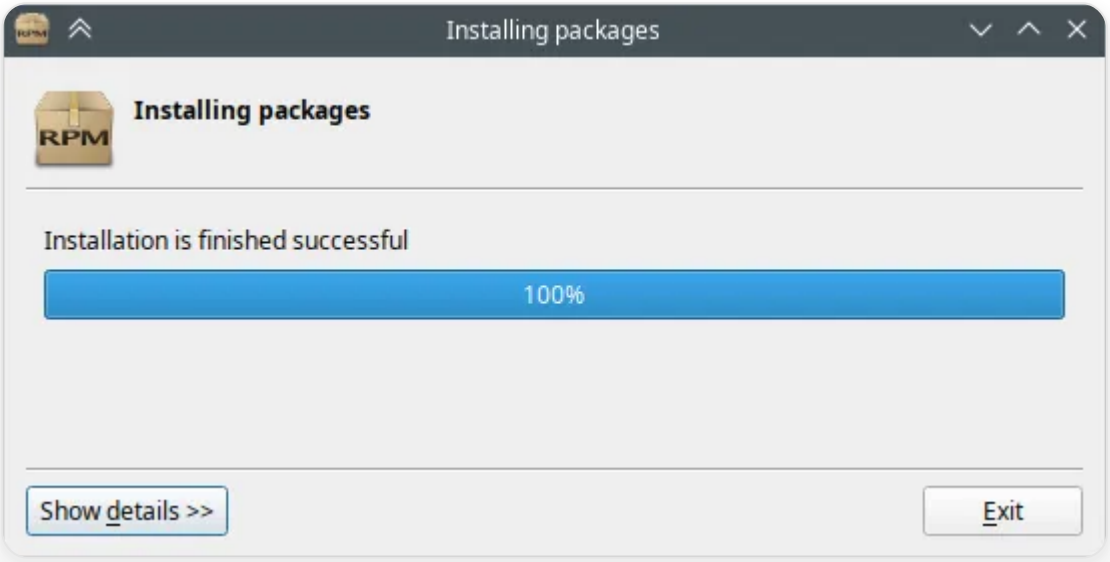
2. Нажмите на кнопку **Установить**.



3. При необходимости укажите пароль системного администратора.



4. Дождитесь окончания установки.



Установка DEB-пакета

Через терминал

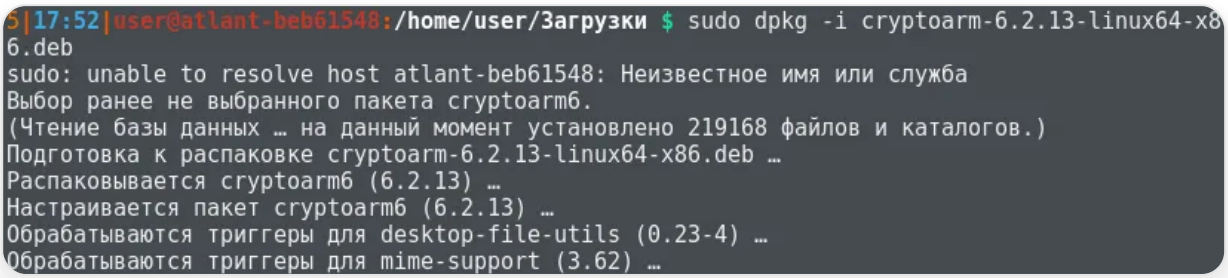
1. Откройте терминал.
2. Выполните команду для установки пакета:
   - Если вы находитесь в той же папке, что и пакет:

```
sudo dpkg -i имя_пакета.deb
```

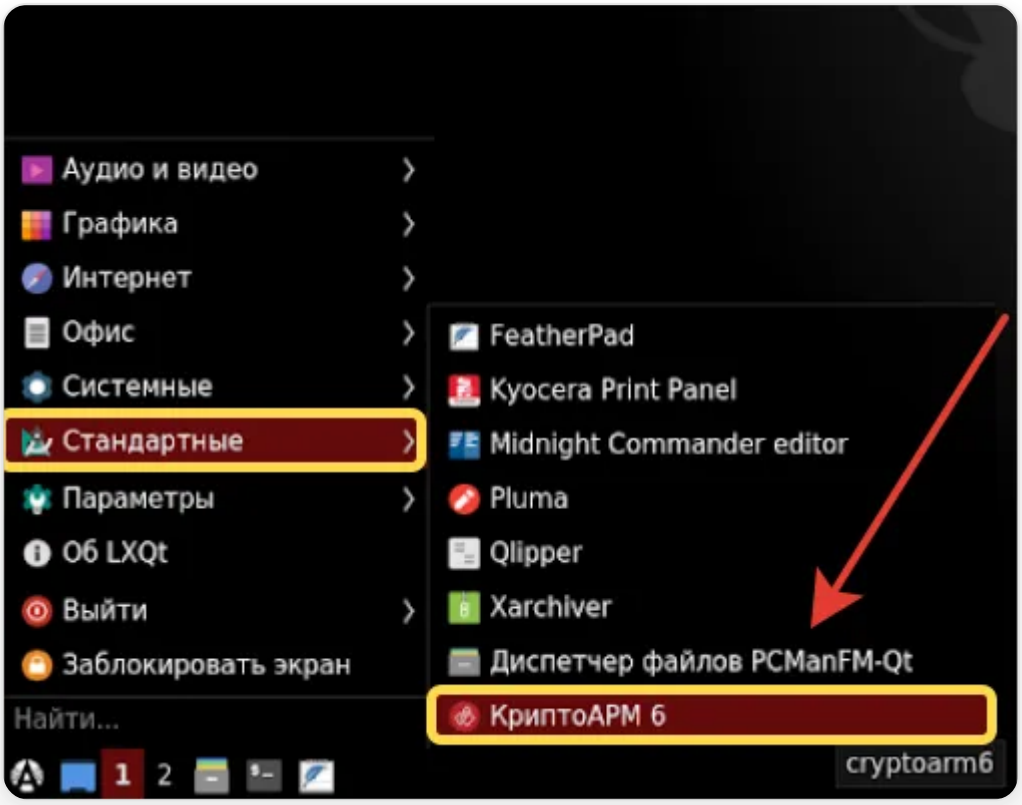
   - Если пакет находится в другой папке:

```
sudo dpkg -i /{путь_до_файла}/имя_пакета.deb
```

3. Дождитесь окончания установки.

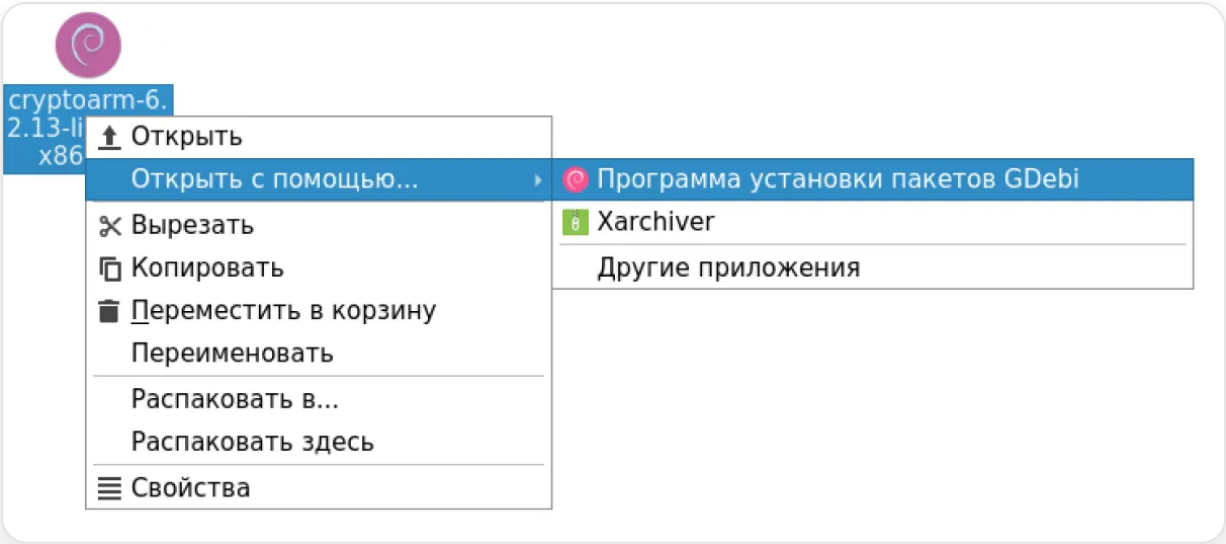


После установки приложение автоматически появляется в меню системы. Например, в ОС «Атлант» приложение можно найти в разделе **Стандартные**.

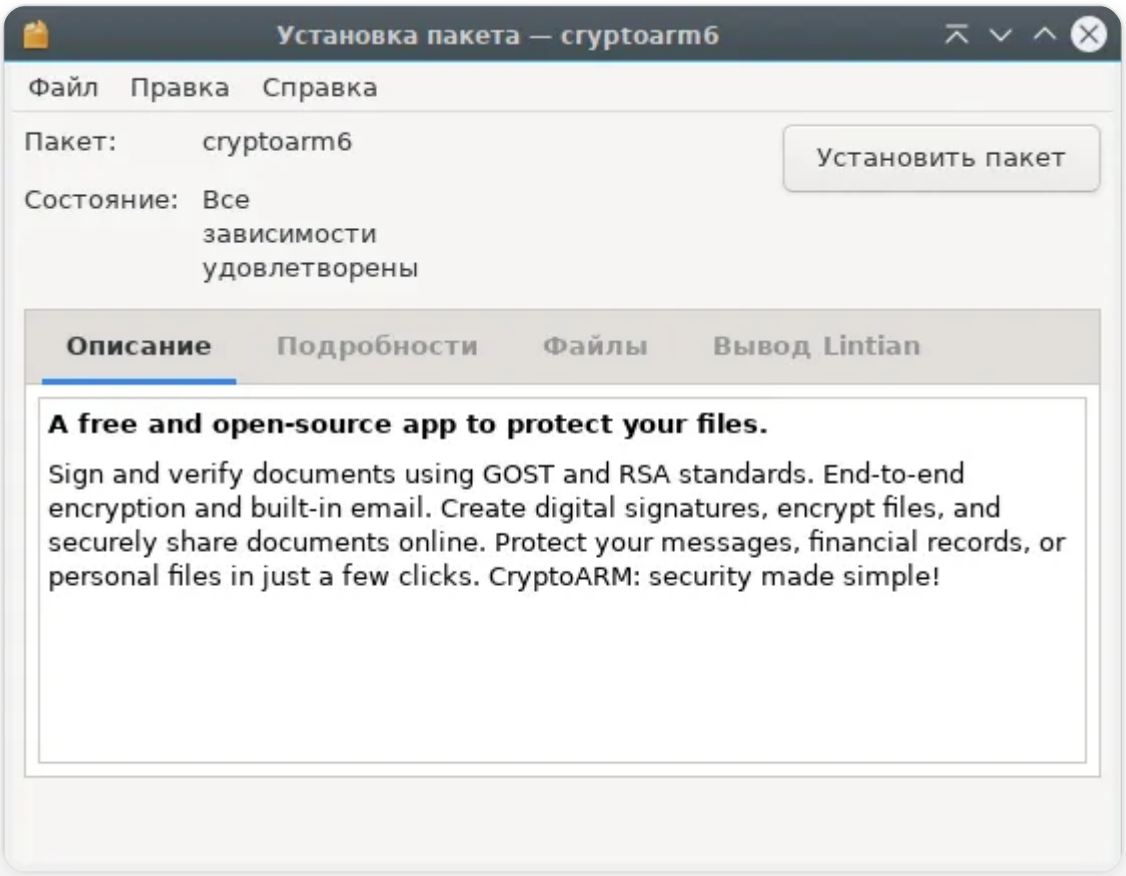


Через графический интерфейс

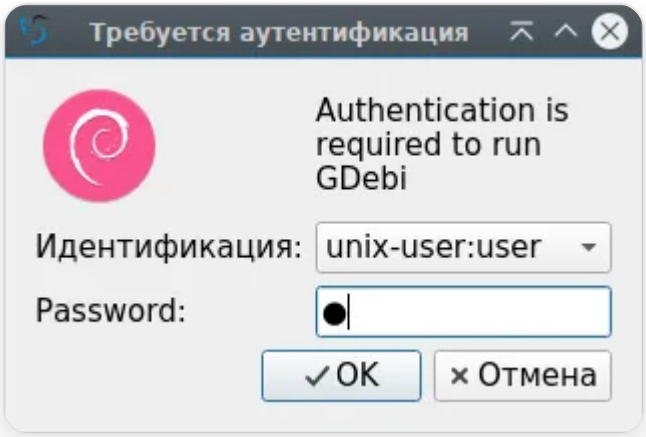
1. Дважды кликните на файл `.deb` или откройте его через установщик пакетов.



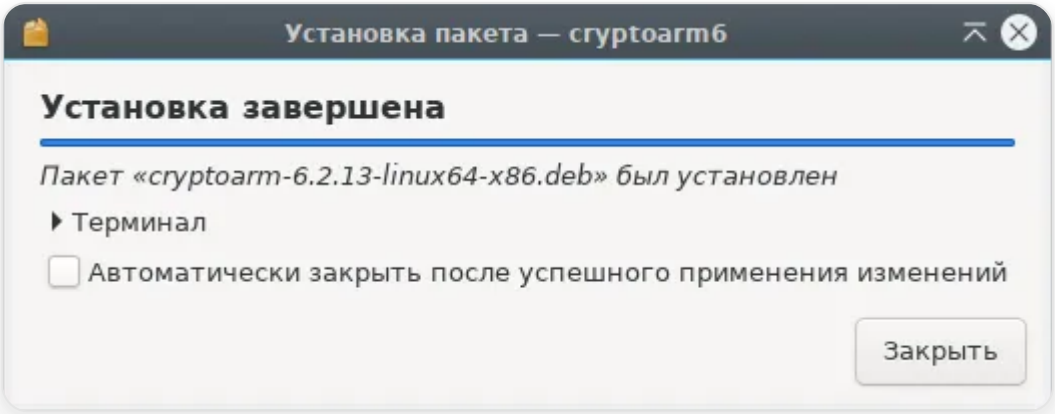
2. Нажмите на кнопку **Установить пакет**.



3. При необходимости укажите пароль системного администратора.



4. Дождитесь окончания установки.



Удаление КриптоАРМ

RPM-пакеты

1. Откройте терминал и переключитесь на `root` при необходимости:

```
su -
```

2. Выполните команду:

   Удаление только приложения:

```
rpm -e имя_пакета
```

   Удаление вместе с зависимостями (если установлено через `apt-get`):

```
apt-get remove имя_пакета
```

После выполнения команды приложение будет удалено из системы.

DEB-пакеты

1. Откройте терминал.
2. Выполните команду:

   Удаление приложения:

   ```
   sudo dpkg -r имя_пакета
   ```

   Полное удаление с настройками:

   ```
   sudo dpkg -P имя_пакета
   ```

После выполнения команды приложение будет удалено из системы.

Открыть статью на сайте

Установка КриптоАРМ на macOS

- Загрузка дистрибутива
- Установка
- Меню приложения КриптоАРМ на macOS

Загрузка дистрибутива

Скачайте установочный файл из официальных источников:

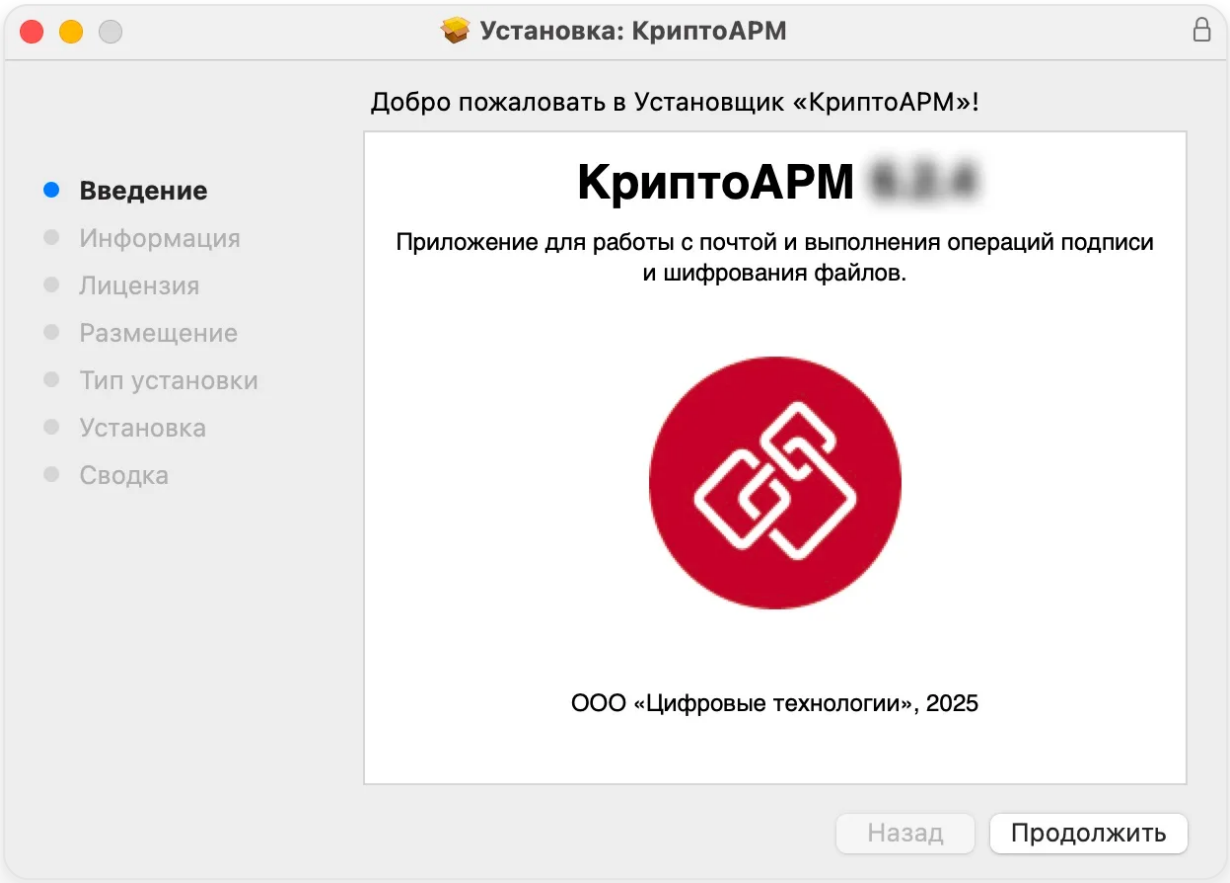
- Официальный сайт КриптоАРМ
- Сайт компании-разработчика Trusted.ru

Установка

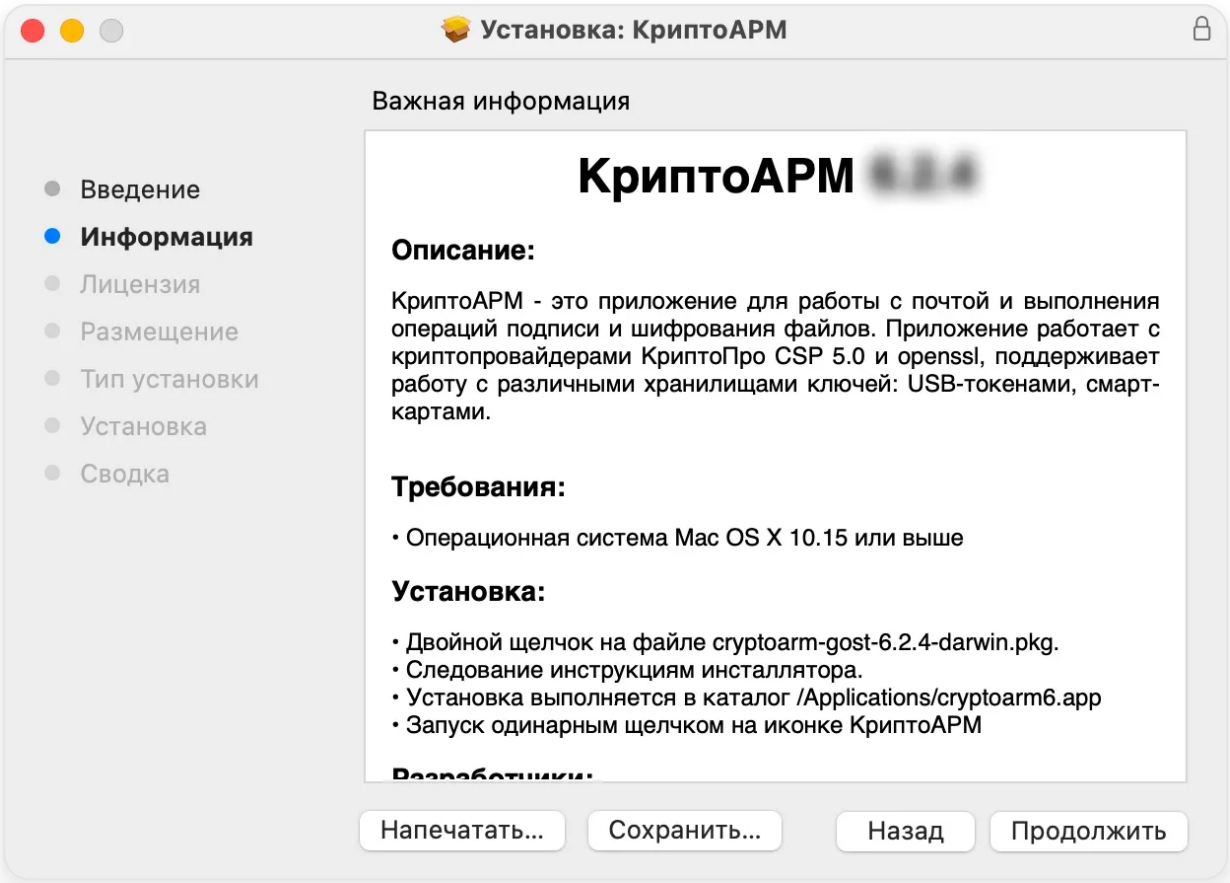
Дистрибутив приложения поставляется в упакованном виде в формате .dmg и представляет собой образ диска, содержащий пакет установки **cryptoarm-x.x.x-x64.pkg,** описание приложения, каталог со скриптами удаления приложения.

1. Для установки пакета через графический интерфейс откройте образ диска с дистрибутивом **cryptoarm-x.x.x-x64.dmg**.
2. Для установки приложения запустите на исполнение файл **cryptoarm-x.x.x-64.pkg**.

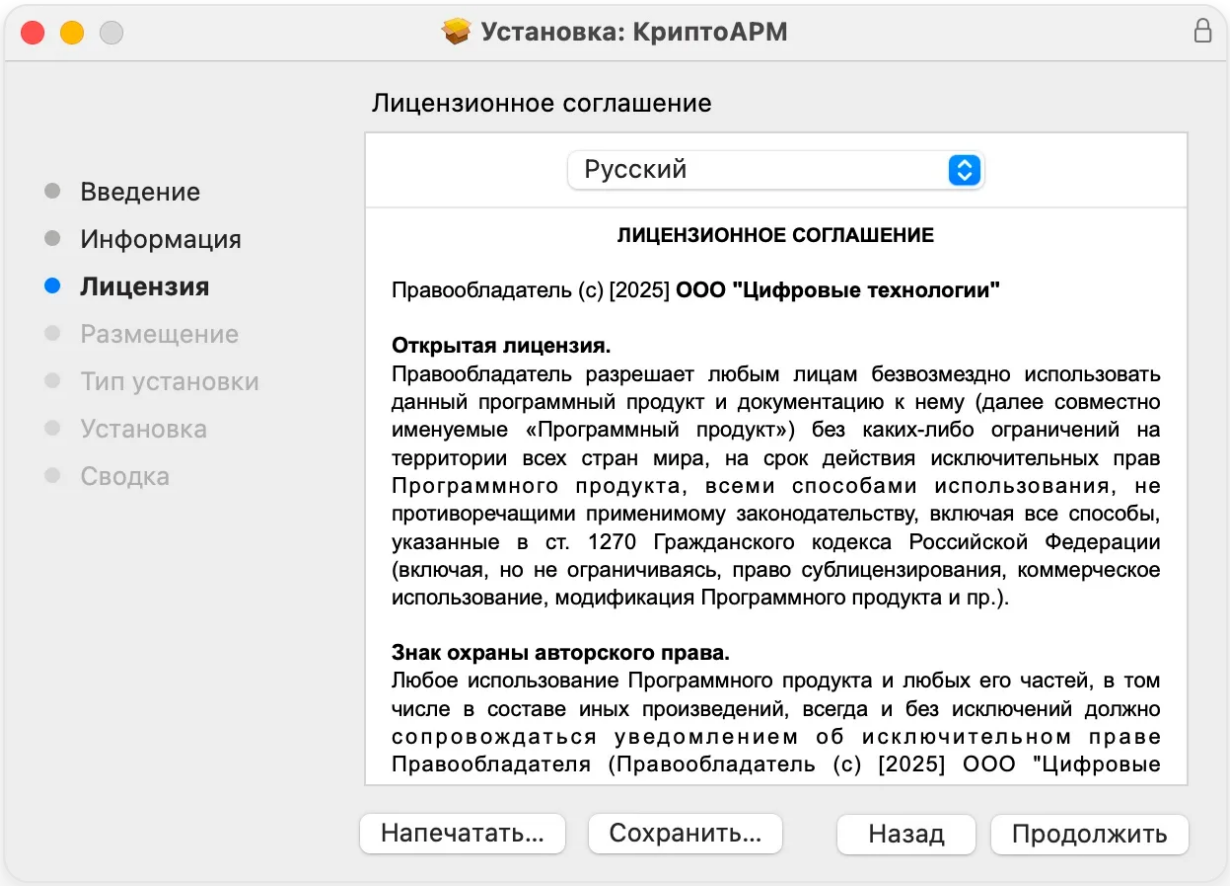
   Установочный пакет для приложения может поставляться вне образа диска. В таком случае нужно сразу запустить файл **cryptoarm-x.x.x-64.pkg** (где x.x.x – номер версии).
3. Откроется мастер установки. Нажмите **Продолжить**.



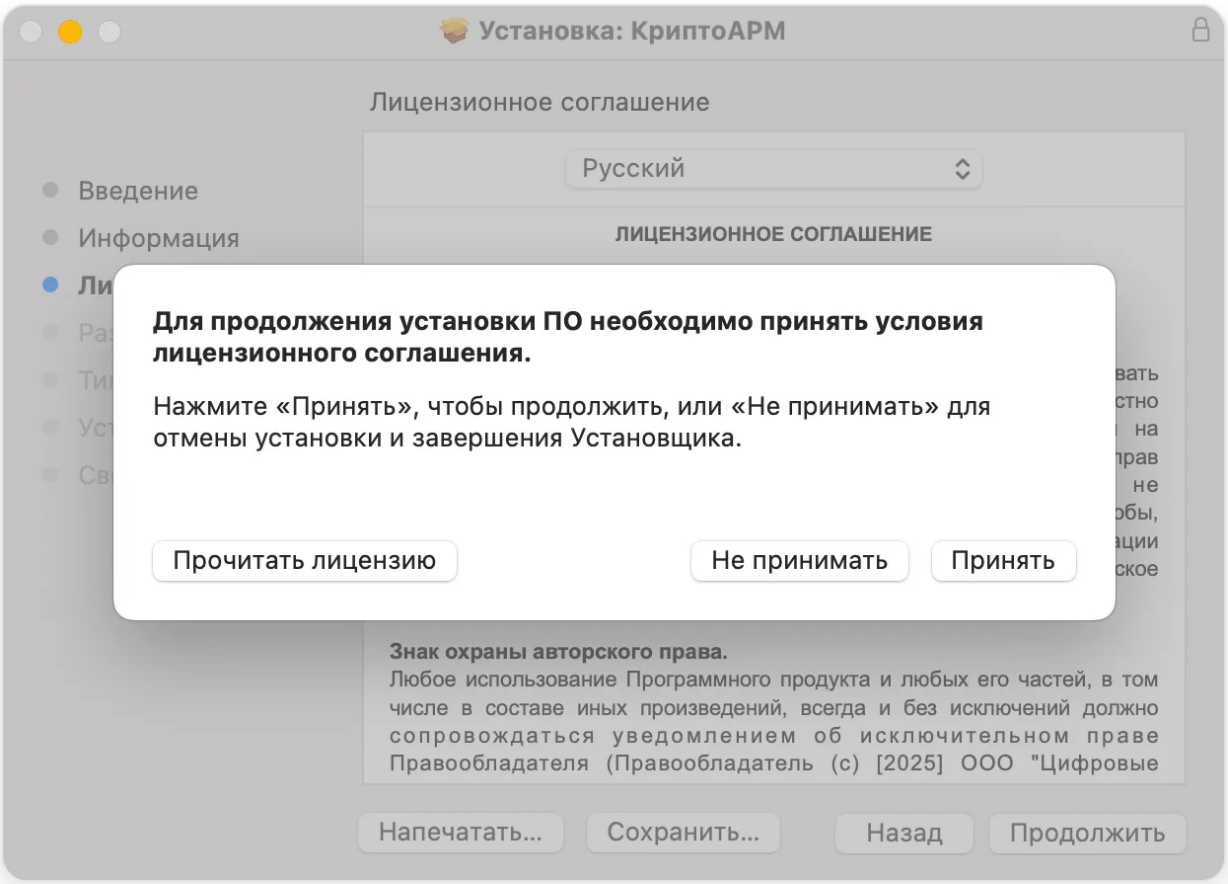
4. Откроется окно с описанием программы. Нажмите **Продолжить**.



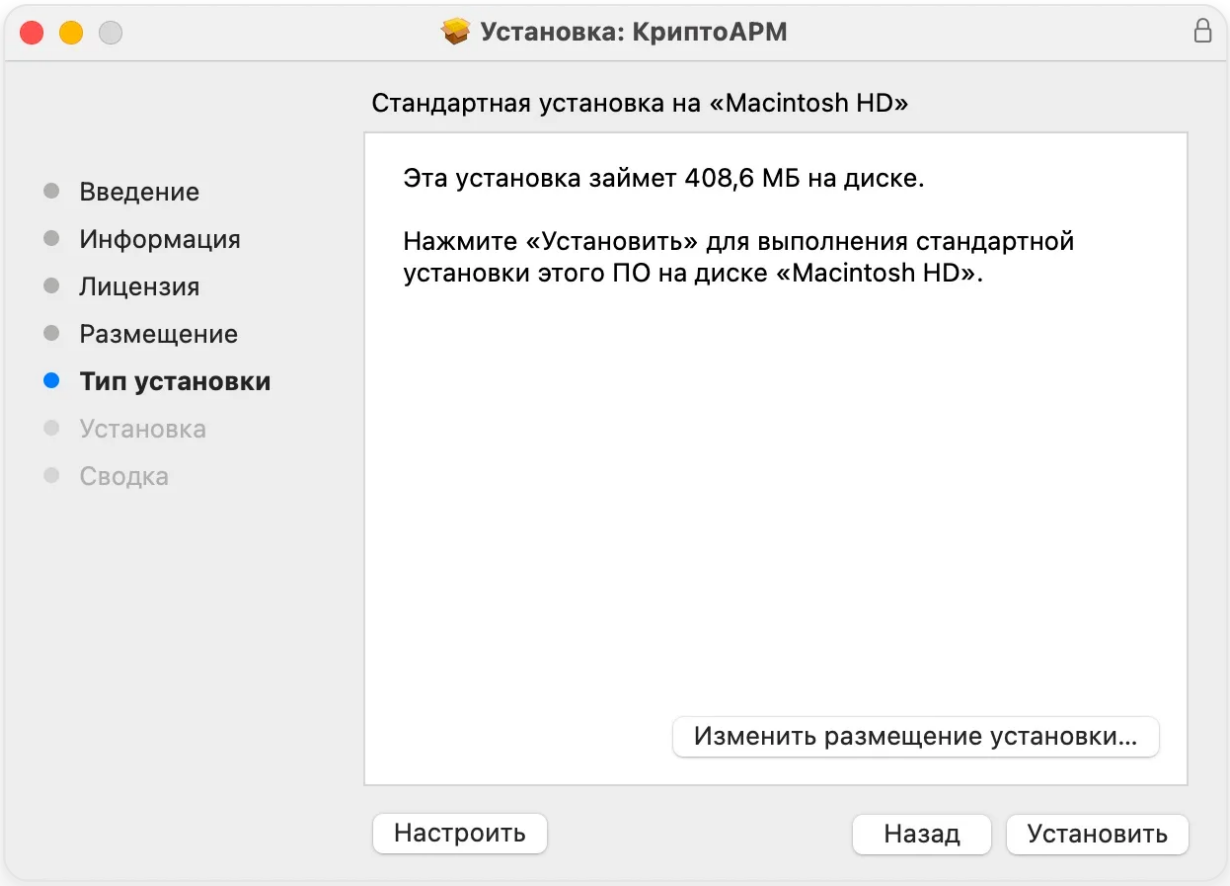
5. Ознакомьтесь с условиями лицензионного соглашения. Нажмите **Продолжить**.



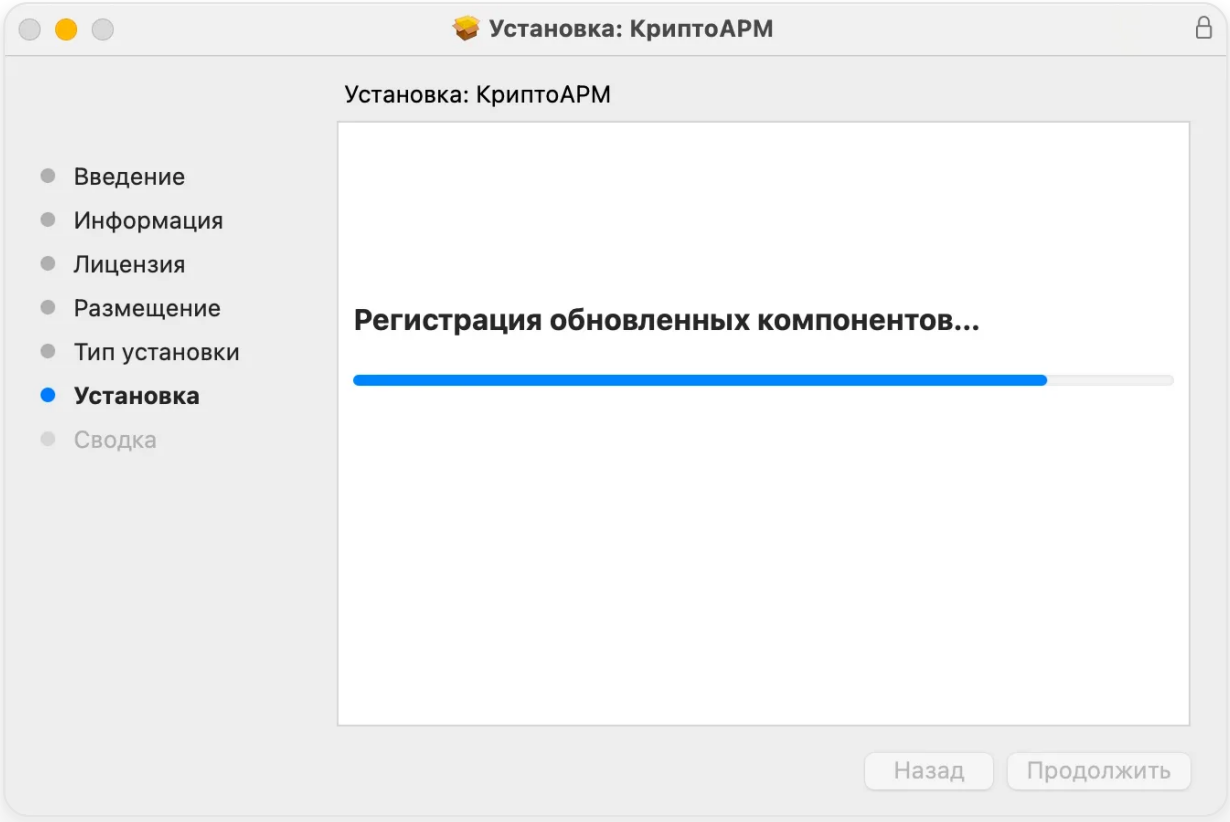
Примите условия лицензионного соглашения по кнопке **Принять**. По кнопке **Не принимать** произойдет отмена установки.



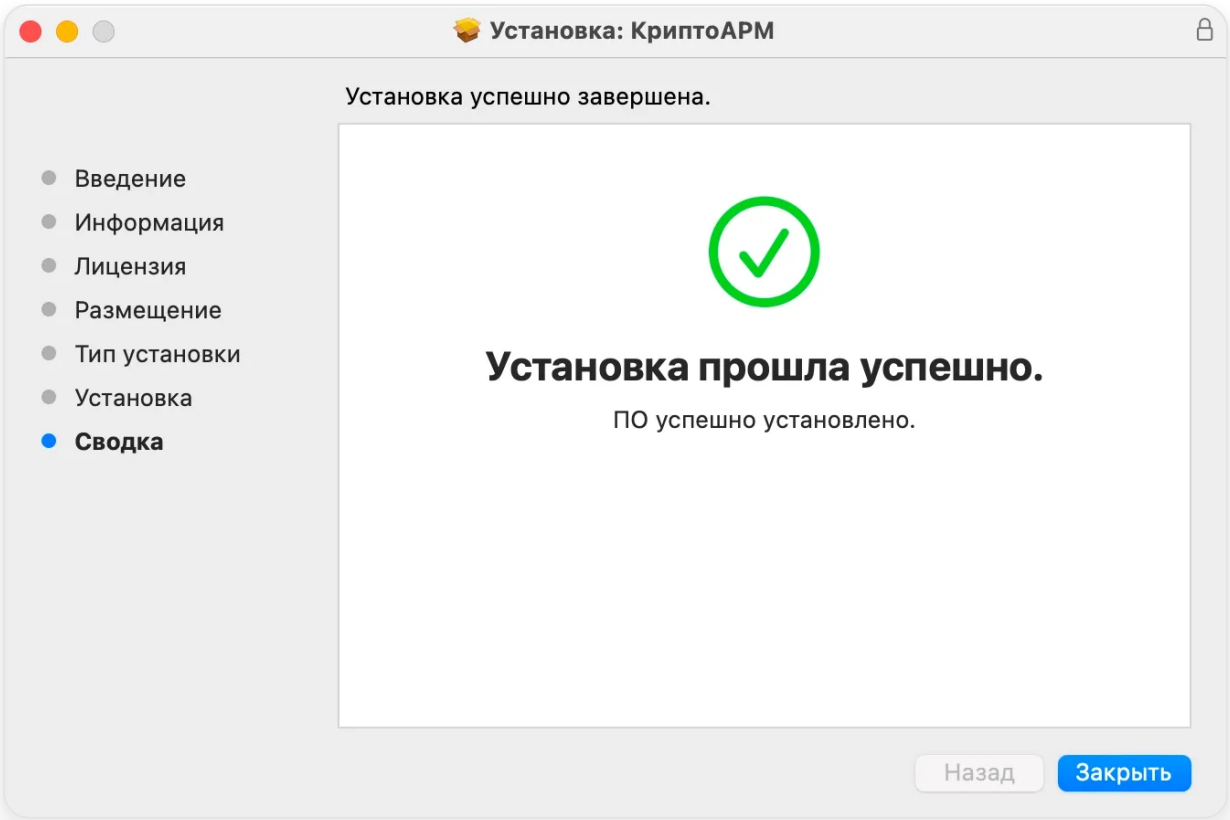
6. На последнем шаге мастера нажмите **Установить** для завершения установки.



Запустится установка программы на компьютер.



7. Закройте окно установки.



После установки программы в **Launchpad** появится ярлык приложения.

В каталоге **Applications** (Программы) будут созданы подкаталоги приложения.

Меню приложения КриптоАРМ на macOS

Приложение КриптоАРМ в macOS имеет стандартное меню, расположенное в верхней части экрана. В зависимости от активного окна, доступны различные пункты.

1. **Меню приложения**

   Содержит общие команды для управления программой:

   - **О программе** – информация о версии КриптоАРМ.
   - **Настройки... (⌘,)** – открывает параметры приложения.
   - **Скрыть КриптоАРМ (⌘H)** – временно убирает окно программы.
   - **Скрыть остальные (⌥⌘H)** – скрывает все приложения, кроме КриптоАРМ.
   - **Выход (⌘Q)** – завершает работу программы.

2. **Меню "Окно"**

Управление открытыми окнами в приложении:

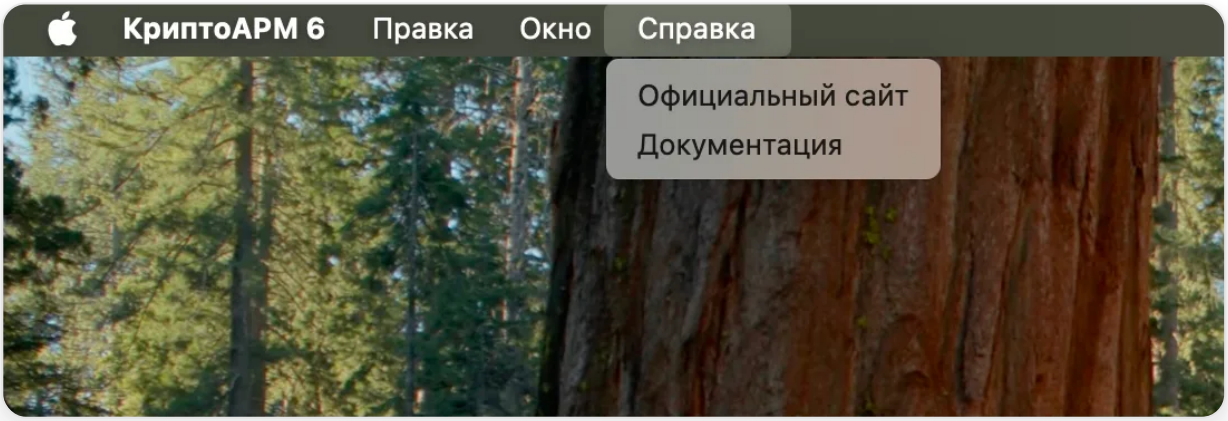
Пункт меню	Горячая клавиша	Описание
Свернуть (⌘M)	`⌘ + M`	Сворачивает текущее окно в Dock.
Развернуть	–	Переводит окно в полноэкранный режим (если поддерживается).
Закрыть (⌘W)	`⌘ + W`	Закрывает текущее окно (не завершает программу).
На передний план	–	Переключает на активное окно КриптоАРМ, если открыто несколько.

```
<img src="../images/install-mac-10.webp" alt="Окончание установки" width="60%">
```

1. **Меню "Справка"**

   Доступ к официальной документации и поддержке:

Пункт	Описание
Официальный сайт	Открывает сайт КриптоАРМ в браузере.
Документация	Открывает руководство пользователя.



Открыть статью на сайте

Установка КриптоПро CSP на Windows

- Загрузка дистрибутива
- Установка

Скачайте дистрибутив с официального сайта компании ООО «КРИПТО-ПРО» или используйте компакт диск. Запустите скачанный файл дистрибутива CSPSetup.exe.

Загрузка дистрибутива

1. Перейдите на официальный сайт КриптоПро.
2. Пройдите регистрацию или авторизацию. Скачивание дистрибутива доступно только после регистрации. Это связано с тем, что криптопровайдер представляет собой средство криптографической защиты информации, а это значит, что его распространение подлежит учету в соответствующих государственных органах.
3. Откроется страница продукта КриптоПро CSP.
4. Нажмите **Скачать**.
5. Ознакомьтесь и согласитесь с лицензионным соглашением.
6. Скачайте дистрибутив в соответствии с установленной операционной системой и её разрядностью.

> ⚠️ **Требования к версии**: КриптоАРМ поддерживает КриптоПро CSP версии 5.0 и выше

Установка

Подготовка

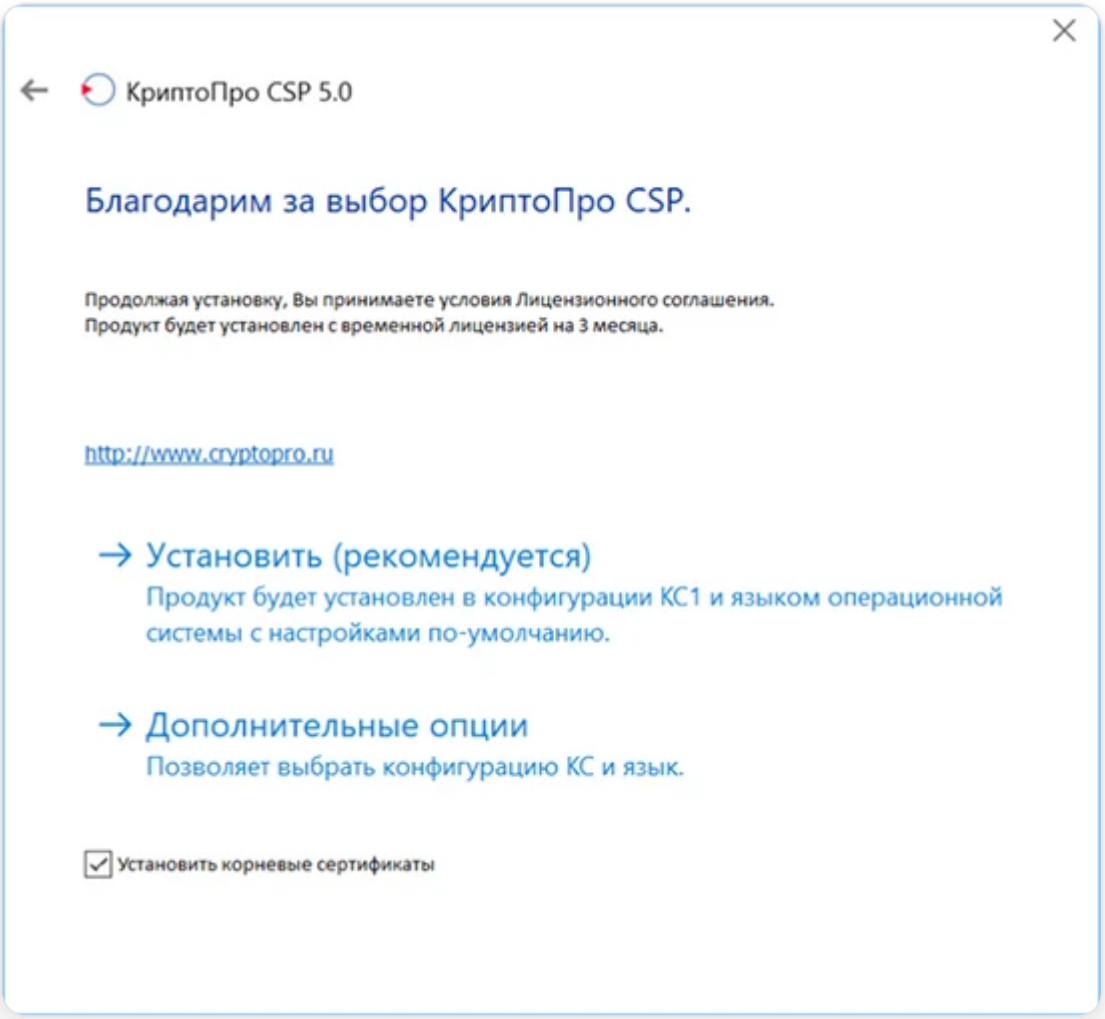
- Убедитесь, что у вас есть права администратора
- Закройте все работающие приложения

Пошаговая установка

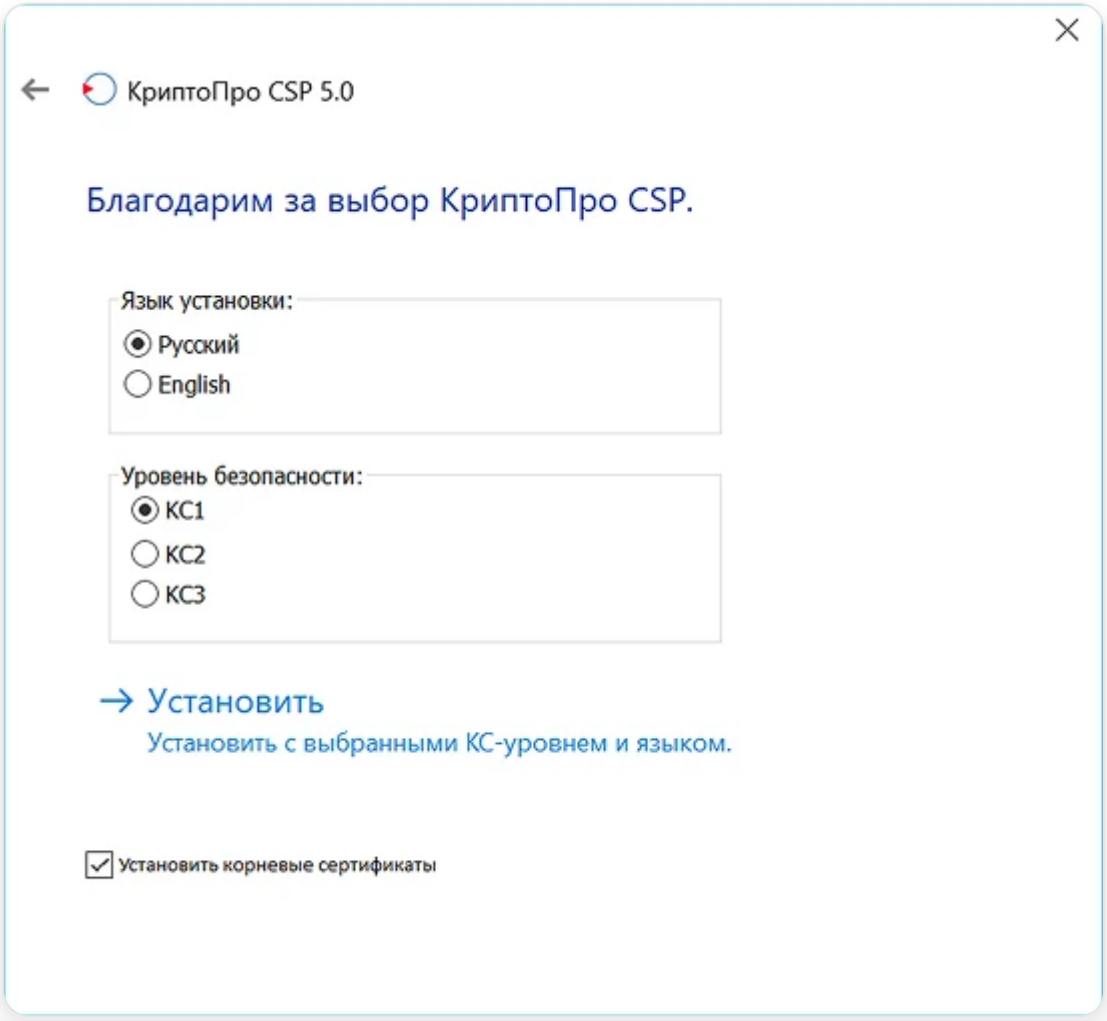
1. Если используется компакт-диск в стартовом меню диска выберите систему и язык установки.



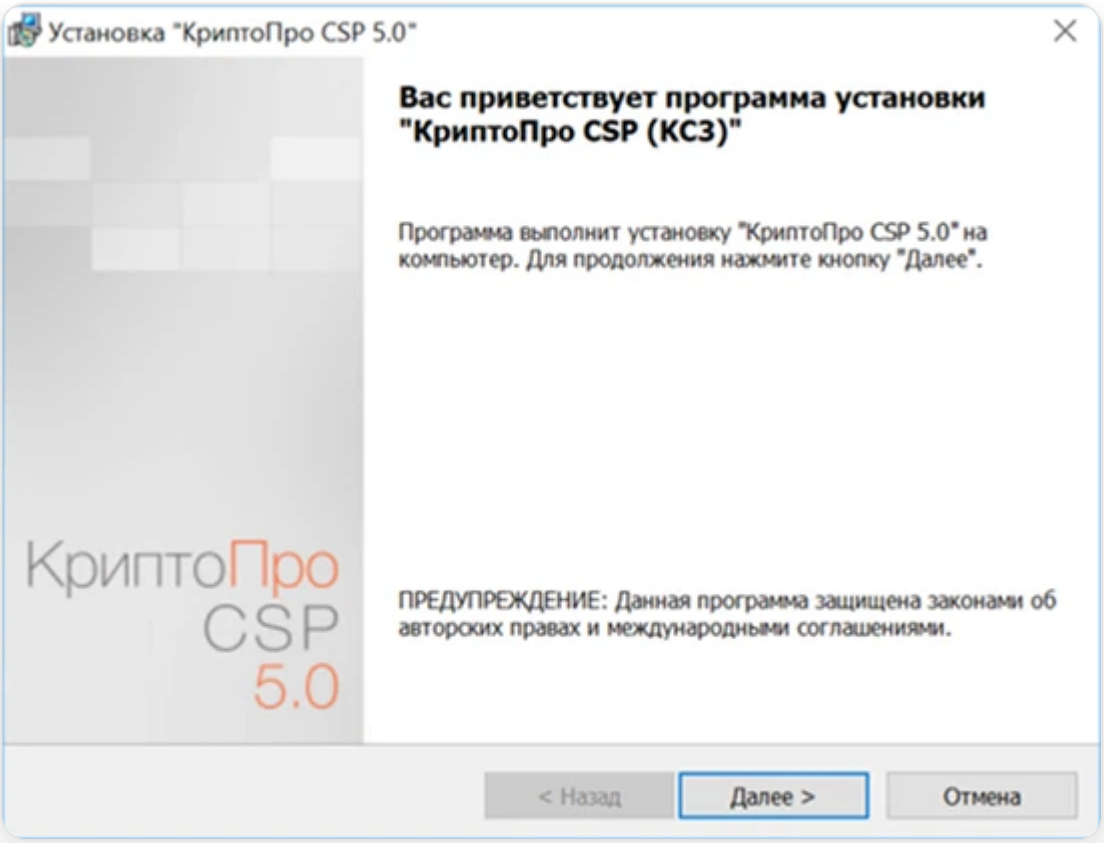
2. Откроется приветственное окно мастера установки КриптоПро CSP. Для изменения уровня класса защиты (КС1/КС2/КС3) или языка установки нажмите кнопку **Дополнительные опции**.



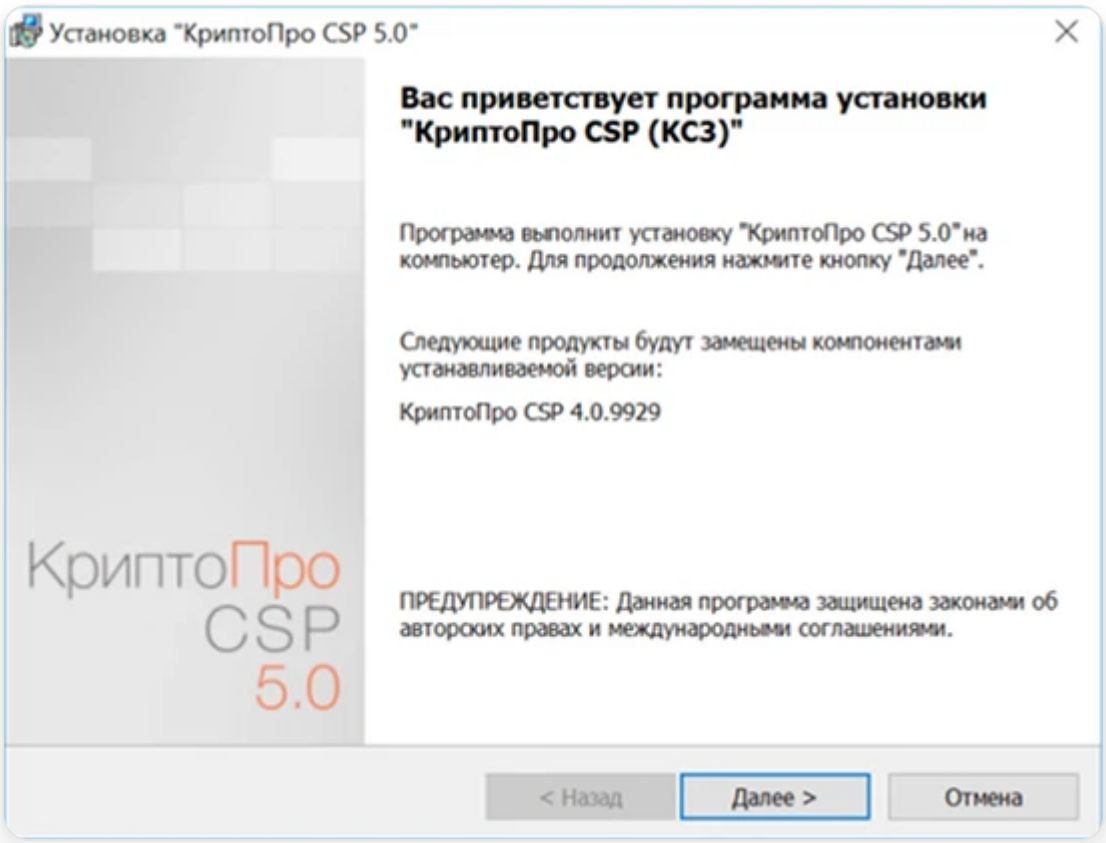
3. В открывшемся окне укажите **Язык установки** и класс защиты в поле **Уровень безопасности**. Нажмите кнопку Установить.



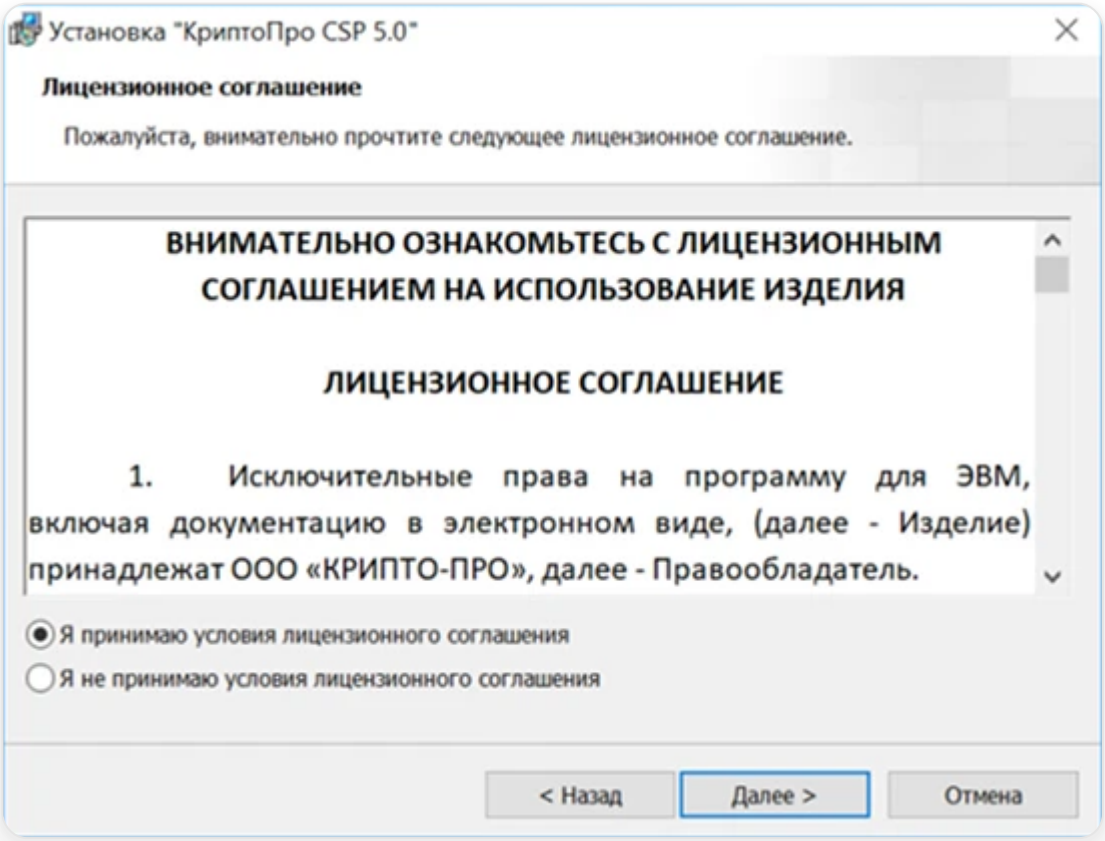
4. Последующая установка производится в соответствии с сообщениями, выдаваемыми программой установки. В процессе установки будет предложено зарегистрировать дополнительные считыватели ключевой информации, дополнительные датчики случайных чисел или настроить криптопровайдер на использование дополнительной защиты. Для продолжения установки нажмите **Далее**.



5. Если в системе была установлена более ранняя версия СКЗИ КриптоПро CSP, то в окне установки появится информация о текущей версии. Для продолжения установки нажмите **Далее**.

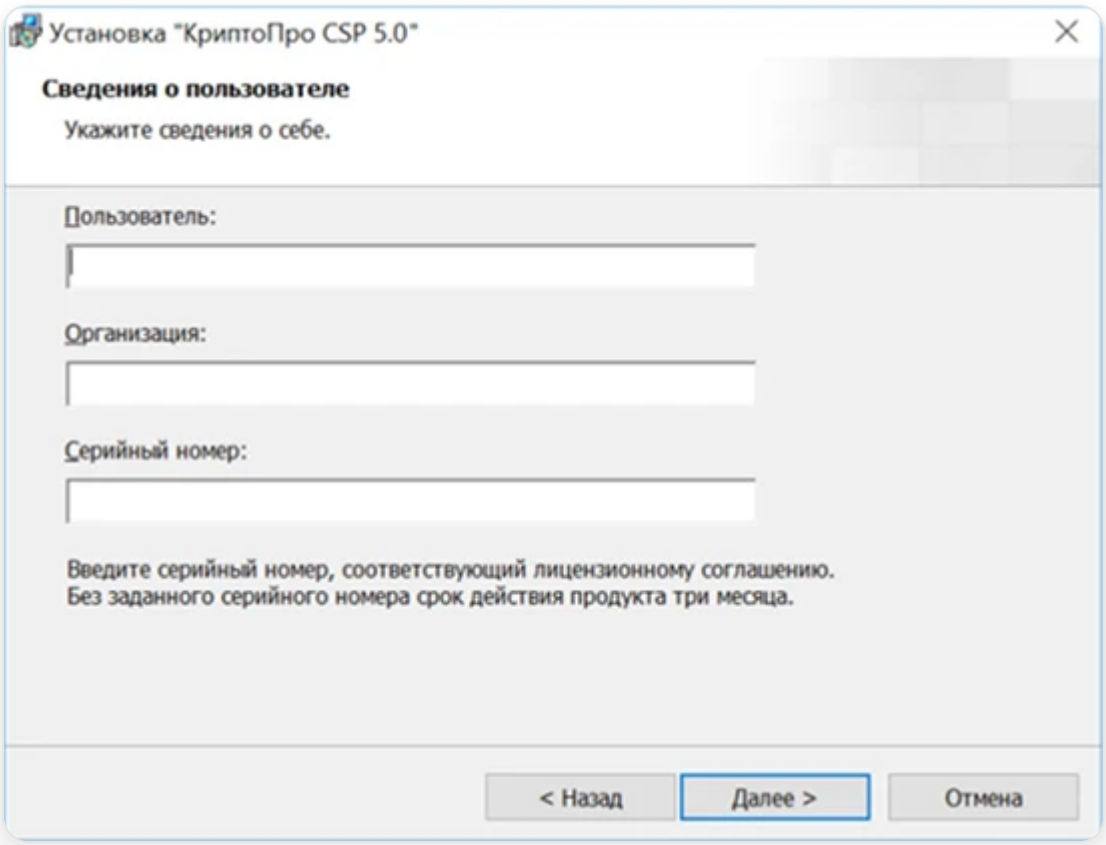


6. Внимательно ознакомьтесь с лицензионным соглашением на использование СКЗИ КриптоПро CSP. Выберите опцию Я принимаю условия лицензионного соглашения и нажмите Далее для продолжения установки.

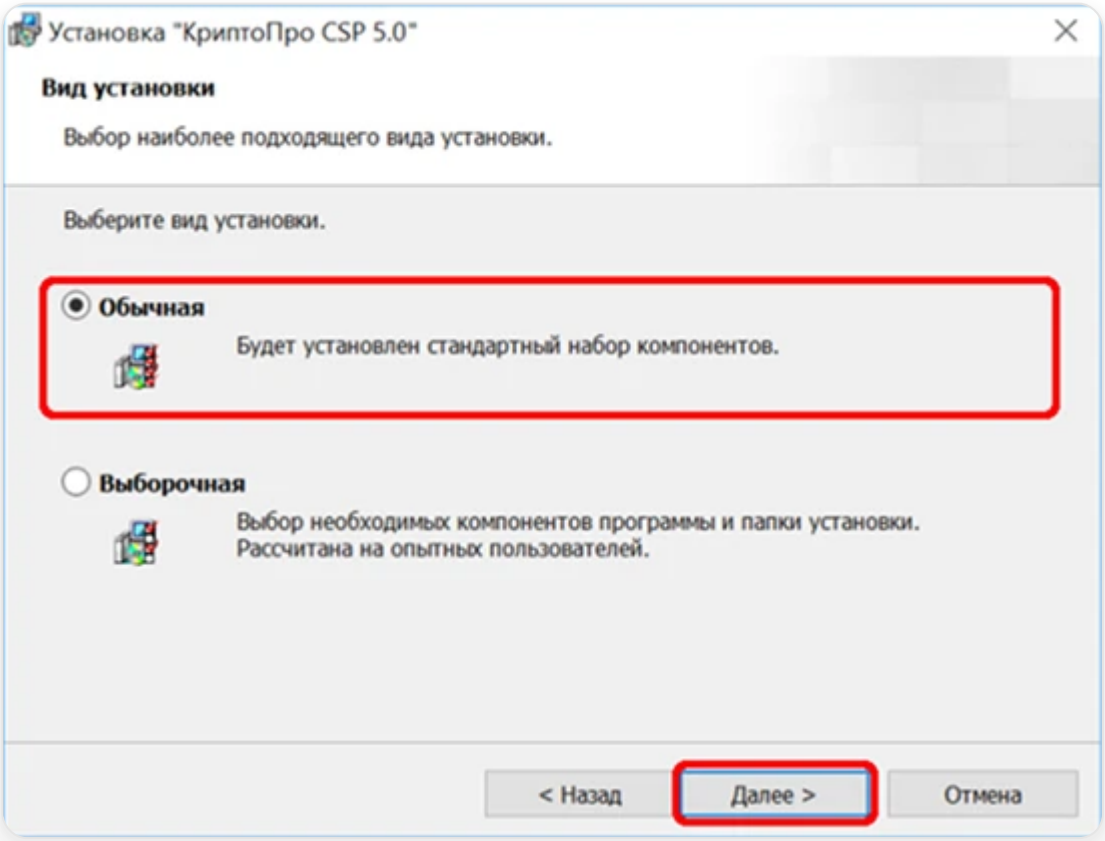


7. В окне сведений о пользователе можно ввести данные о пользователе, организации и серийный номер лицензии. Эти данные можно вести позже в процессе работы с программой. Для продолжения установки нажмите **Далее**.

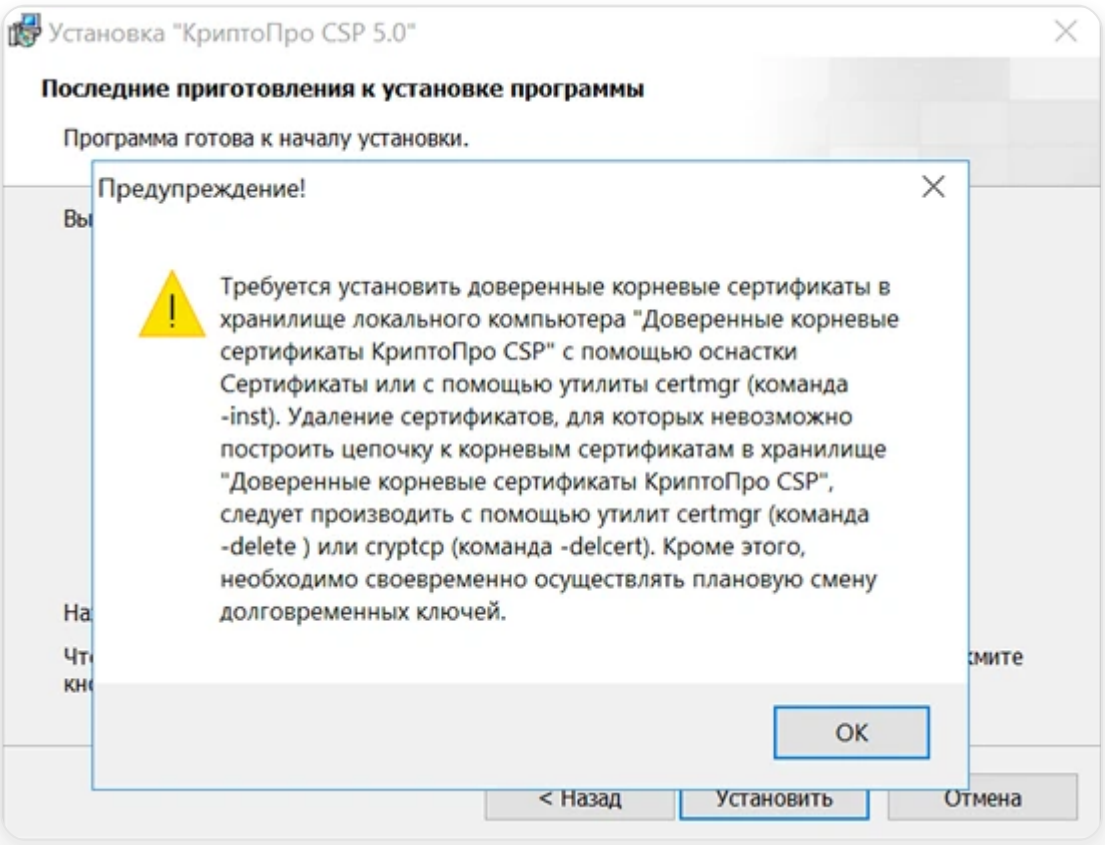
> ⚠️ **Примечание**: Без введённого серийного номера СКЗИ КриптоПро CSP будет работать в тестовом режиме в течение трёх месяцев.



8. Выберите тип установки: **Обычная** — основные файлы для работы СКЗИ. Для продолжения установки нажмите **Далее**.



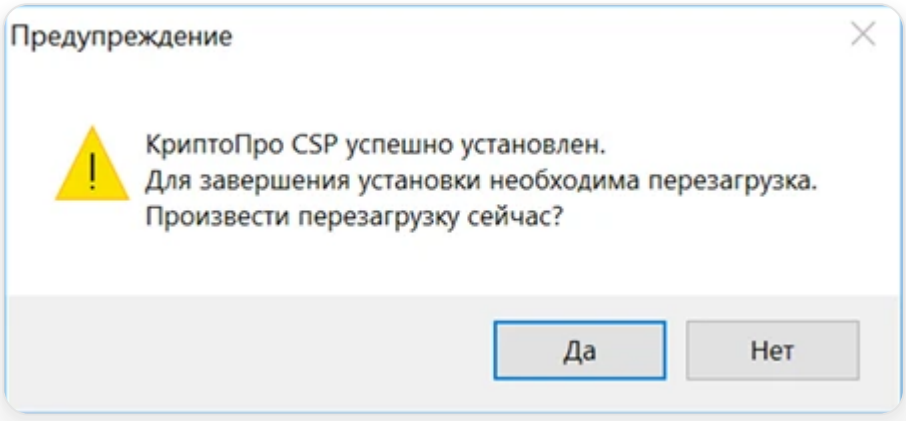
9. В случае выбора опции усиленного контроля использования ключей появится окно предупреждения с перечнем необходимых действий для корректной настройки СКЗИ КриптоПро CSP, нажмите **OK**.



10. Начнётся процесс установки, в окне мастера установки отобразится прогресс.

11. При завершении установки всех компонентов отобразится окно с информацией об успешной установке КриптоПро CSP. Нажмите кнопку **Готово** для выхода из программы установки.

12. Нажмите кнопку **Да** для перезагрузки системы и завершения установки с применением изменений криптопровайдера КриптоПро CSP.



Открыть статью на сайте

Установка КриптоПро CSP на Linux

- Загрузка дистрибутива
- Установка КриптоПро CSP
- Установка пакета для графического интерфейса ввода пароля
- Установка пакетов для работы с ключевыми носителями
- Установка лицензии КриптоПро CSP
- Установка модулей TSP и OCSP
- Установка лицензии на модули TSP и OCSP
- Настройки для работы с КриптоПро CSP 4

Загрузка дистрибутива

1. Перейдите на официальный сайт КриптоПро.
2. Пройдите регистрацию или авторизацию. Скачивание дистрибутива доступно только после регистрации. Это связано с тем, что криптопровайдер представляет собой средство криптографической защиты информации, а это значит, что его распространение подлежит учету в соответствующих государственных органах.
3. На странице продукта КриптоПро CSP нажмите **Скачать**.
4. Ознакомьтесь и согласитесь с лицензионным соглашением.
5. Скачайте дистрибутив `.tgz` в соответствии с установленной операционной системой и её разрядностью.

> ⚠️ **Требования к версии**: КриптоАРМ поддерживает КриптоПро CSP версии 5.0 и выше

Установка КриптоПро CSP

> ⚠️ **Примечание**: Все действия выполняются от имени пользователя с правами администратора `root` или через `sudo`.

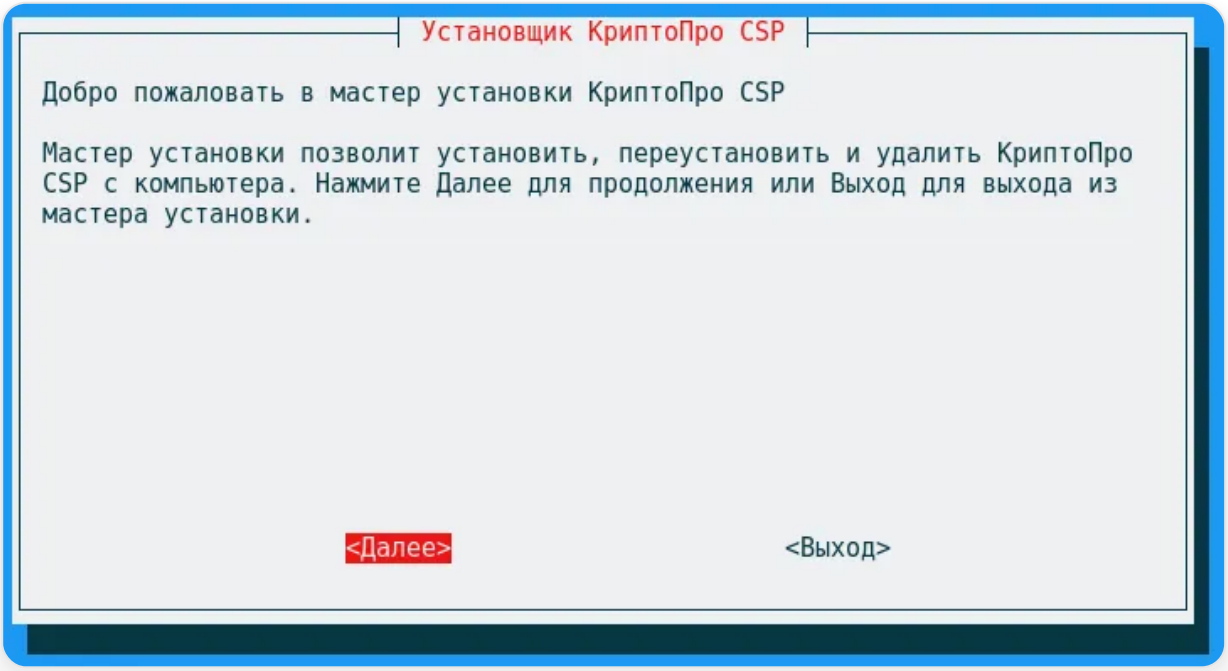
1. Если дистрибутив скачан в формате .tgz, его необходимо распаковать. Сделать это можно двумя способами — через графический интерфейс или в терминале.
    - Найдите архив в файловом менеджере и нажмите на него правой кнопкой мыши. Выберите пункт **Распаковать в эту папку**/**Извлечь здесь**.
    - Выполните команду в терминале:

```
tar -xzf имя_пакета.tgz # Распаковка в текущую директорию
tar -xzf имя_пакета.tgz -C  /{путь_до_файла}/ # Распаковка в указанную директорию
```

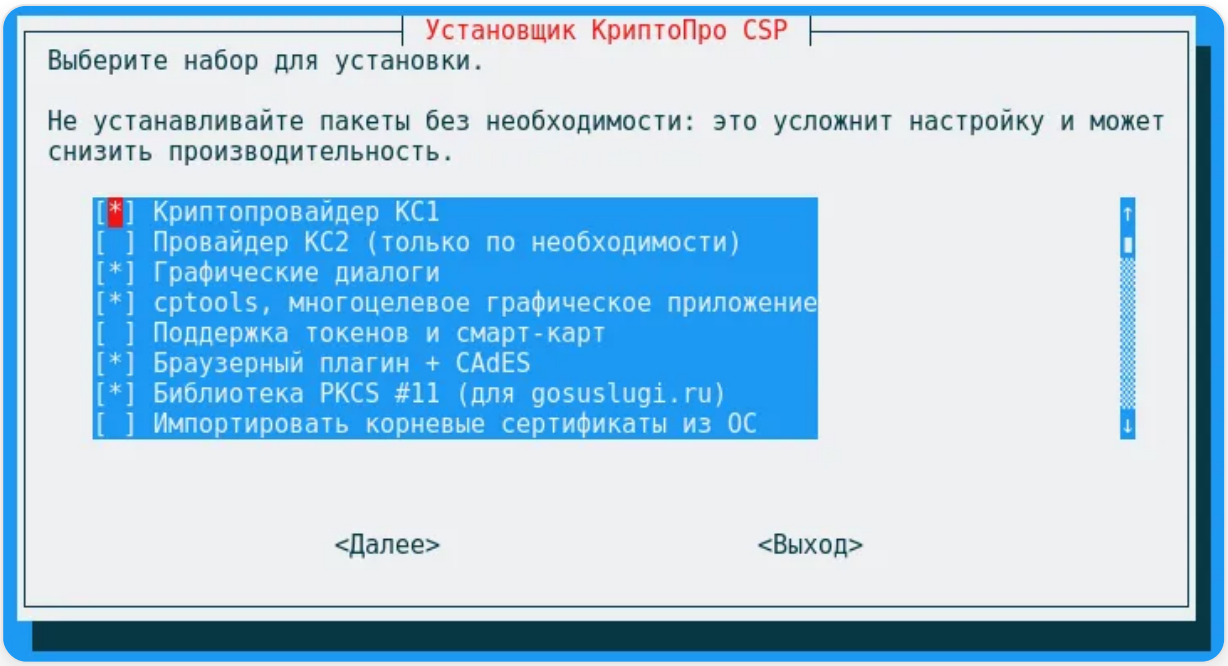
2. Запустите установщик по команде:

```
/{путь_до_файла}/install_gui.sh # Запуск графического установщика
/{путь_до_файла}/install.sh # Без графического установщика
```

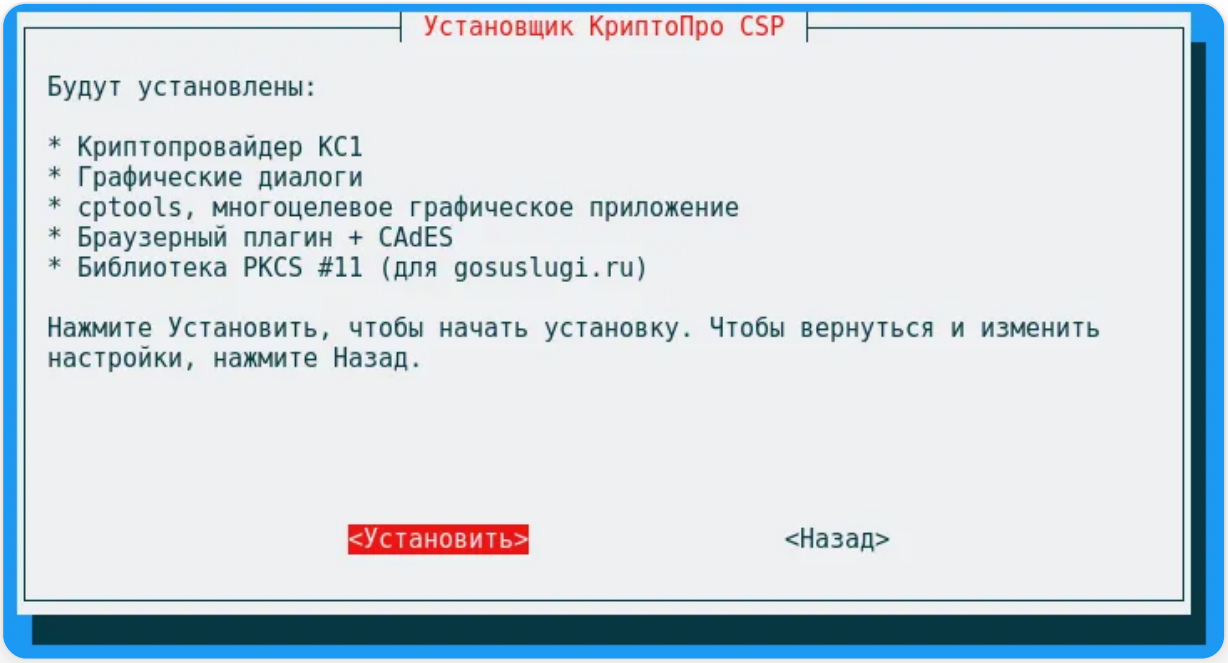
3. Если запущена графическая установка, нажмите **Далее** в открывшемся окне.



4. Выберите все дополнительные пакеты, кроме «Провайдер КС2», и снова нажмите **Далее**.



5. Подтвердите установку и дождитесь её окончания.



6. Закройте установщик.

> 📌 По умолчанию CSP устанавливается в /opt/cprocsp/.

Установка пакета для графического интерфейса ввода пароля

Для работы с контейнерами закрытых ключей требуется ввод пароля.

Установите пакет для графического интерфейса диалога ввода пароля, запустив в терминале команду:

```
sudo dpkg -i /<путь_до_файла>/cprocsp-rdr-gui-<версия>.deb
```

Установка пакетов для работы с ключевыми носителями

> ⚠️ **Примечание**: Для работы с ключевыми ностителями в deb-based системе должны быть установлены:
>
> - библиотека `libccid` не ниже 1.3.11,
> - пакеты `pcscd` и `libpcsclite1`.

1. Установите пакеты и драйвера для работы с ключевыми носителями с помощью команд в терминале:

   ```
   sudo dpkg -i <путь_до_файла>/cprocsp-rdr-pcsc-<...>.deb
   ```

2. Для ключевого носителя **Рутокен**:

   ```
   sudo dpkg -i <путь_до_файла>/cprocsp-rdr-rutoken-<...>.deb
   ```

   ```
   sudo dpkg -i <путь_до_файла>/ifd-rutokens_<...>.deb
   ```

3. Для ключевого носителя **JaCarta**:

   ```
   sudo dpkg -i <путь_до_файла>/cprocsp-rdr-jacarta -<...>.deb
   ```

4. Для ключевого носителя **ESMART**:

   ```
   sudo dpkg -i <путь_до_файла>/cprocsp-rdr-esmart -<...>.deb
   ```

Установка лицензии КриптоПро CSP

Установить лицензию можно в разделе Настройки приложения КриптоАРМ или в терминале системы.

1. Откройте терминал.
2. Введите лицензию командой:

```
sudo /opt/cprocsp/sbin/amd64/cpconfig -license -set <серийный_номер>
```

> ⚠️ **Примечание**: Серийный номер вводится с учётом регистра символов.

Установка модулей TSP и OCSP

Для создания подписи со штампом времени или усовершенствованной подписи необходимо установить библиотеки поддержки модулей TSP и OCSP:

1. Скачайте архив **КриптоПро ЭЦП SDK 2.0** по ссылке. Как и в случае с дистрибутивом КриптоПро CSP, для скачивания может потребоваться регистрация.
2. Распакуйте архив.
3. Установите пакет:

```
sudo dpkg -i <путь_до_файла>/cprocsp-pki-x.x.x-amd64-cades.deb
```

Для создания подписи со штампом времени или усовершенствованной подписи необходима установка лицензии на модули TSP и/или OCSP.

Для проверки подписи лицензии на данные модули устанавливать не нужно.

Установка лицензии на модули TSP и OCSP

1. Откройте терминал.
2. Введите лицензию на модуль TSP командой:

```
sudo /opt/cprocsp/bin/amd64/tsputil license -s <серийный_номер>
```

3. Введите лицензию на модуль OCSP командой:

```
sudo /opt/cprocsp/bin/amd64/ocsputil license -s <серийный_номер>
```

> ⚠️ **Примечание**: Серийный номер следует вводить с соблюдением регистра символов.

Настройки для работы с КриптоПро CSP 4

1. Установите пакет cprocsp-rsa из дистрибутива КриптоПро:

```
sudo dpkg -i <путь_до_файла>/cprocsp-rsa-<...>.deb
```

2. Скачайте скрипт.

3. В терминале введите команду:

```
chmod u+x <путь к скрипту>/script.sh  # Делаем скрипт исполняемым
```

4. Далее введите команду:

```
sudo bash <путь к скрипту>/script.sh # Запуск скрипта с правами администратора
```

В результате выполнения команды должно выйти сообщение «Operations done».

Открыть статью на сайте

Установка КриптоПро CSP на macOS

- Загрузка дистрибутива
- Установка КриптоПро CSP
- Установка модулей TSP и OCSP
- Активация лицензий на модули TSP и OCSP в терминале

Загрузка дистрибутива

1. Перейдите на официальный сайт КриптоПро.
2. Пройдите регистрацию или авторизацию. Скачивание дистрибутива доступно только после регистрации. Это связано с тем, что криптопровайдер представляет собой средство криптографической защиты информации, а это значит, что его распространение подлежит учету в соответствующих государственных органах.
3. Откроется страница продукта КриптоПро CSP.
4. Нажмите **Скачать**.
5. Ознакомьтесь и согласитесь с лицензионным соглашением.
6. Скачайте дистрибутив в соответствии с установленной операционной системой и её разрядностью.

> ⚠️ **Требования к версии**: КриптоАРМ поддерживает КриптоПро CSP версии 5.0 и выше

Установка КриптоПро CSP

1. Распакуйте загруженный файл **macos-uni.tgz**.
2. Перейдите в распакованную папку.

> ⚠️ **Примечание**: Установка осуществляется от имени пользователя, имеющего права администратора: под учётной записью `root` или с использованием команды `sudo`.

При установке КриптоПро CSP сначала устанавливается провайдер, затем устанавливаются остальные модули, входящие в состав комплектации.

В ОС Mac OS X для установки ПО применяются пакеты (packages). Пакет – архив дистрибутива, содержащий файлы устанавливаемого приложения и файлы, использующиеся инсталлятором для конфигурирования среды.

Дистрибутив поставляется в упакованном виде, имеет формат .dmg и представляет собой образ диска, содержащий пакет. Для установки пакета откройте двойным щелчком образ диска с дистрибутивом (dmg).

3. Вызовите контекстное меню для файла .dmg и выберите в меню **Открыть**.
4. В открывшемся окне вызовите контекстное меню для файла .pkg и выберите в меню **Открыть**.
5. Появится окно с предупреждением. Нажмите **Продолжить**.
6. В следующем окне нажмите **Разрешить**.
7. Ознакомьтесь и примите лицензионное соглашение и продолжите установку.
8. Выберете все установочные пакеты и нажмите **Продолжить — Установить**.
9. После завершения установки закройте мастер установки.

Установка модулей TSP и OCSP

Для создания подписи со штампом времени или усовершенствованной подписи необходимо установить библиотеки поддержки модулей TSP и OCSP.

Скачать архив для **MacOS** можно по ссылке КриптоПро ЭЦП SDK 2.0. Как и в случае с дистрибутивом КриптоПро CSP, для скачивания может потребовать регистрация.

Установите пакет **cprocsp-pki-x.x.x.pkg**, следуя инструкциям на каждом шагу установщика.

Для создания подписи со штампом времени или усовершенствованной подписи необходима установка лицензии на модули TSP и/или OCSP. Установить лицензии можно в разделе Настройка приложения КриптоАРМ или в терминале системы.

Для создания классической подписи без штампа времени лицензии на данные модули устанавливать не нужно.

Активация лицензий на модули TSP и OCSP в терминале

Для активации лицензий КриптоПро TSP Client и КриптоПро OCSP Client необходимо использовать в Терминале команды вида:

```
sudo /Applications/CryptoPro_ECP.app/Contents/MacOS/bin/tsputil license -s XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

```
sudo /Applications/CryptoPro_ECP.app/Contents/MacOS/bin/ocsputil license -s XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

где вместо **XXXXX-XXXXX-XXXXX-XXXXX-XXXXX** необходимо указать серийный номер приобретенной лицензии КриптоПро TSP Client и КриптоПро OCSP Client.

При появлении строки **Password** необходимо ввести пароль пользователя macOS (символы вводимого пароля не отображаются) и нажать **Enter**.

Проверить статус лицензий можно командами:

```
/Applications/CryptoPro_ECP.app/Contents/MacOS/bin/tsputil license
```

```
/Applications/CryptoPro_ECP.app/Contents/MacOS/bin/ocsputil license
```

Открыть статью на сайте

Проверка атрибута KeyAgreement

- Зачем нужна проверка
- Включение проверки KeyAgreement

Зачем нужна проверка

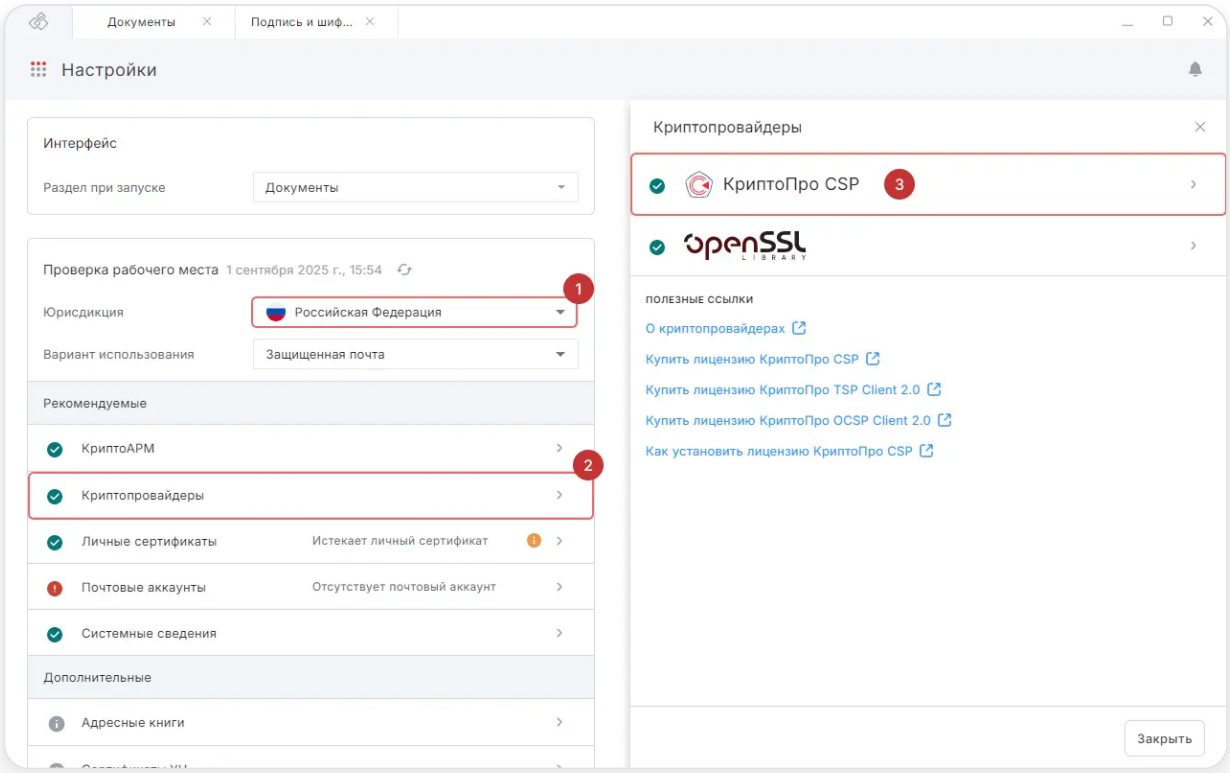
Атрибут **KeyAgreement** (согласование ключей) в расширении **keyUsage** указывает, что сертификат можно использовать для безопасного обмена ключами при шифровании.

- Если проверка включена, операция шифрования возможна только для сертификатов с атрибутом **KeyAgreement**.
- Если проверка отключена, допускается использование сертификатов с атрибутом **keyEncipherment** даже без «согласования ключей».

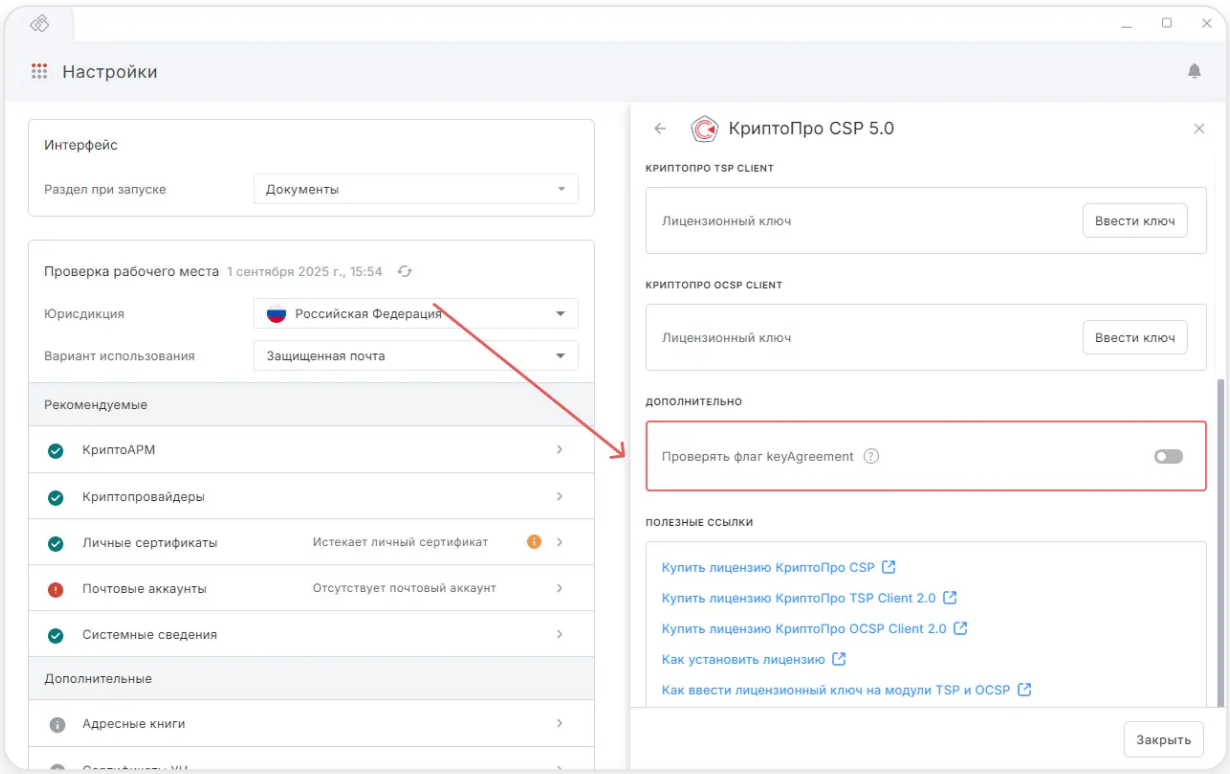
По умолчанию проверка **KeyAgreement** отключена.

Включение проверки KeyAgreement

1. Перейдите в раздел **Настройки**.
2. При необходимости запустите проверку для юрисдикции **Российская Федерация**.
3. Нажмите на панель **Криптопровайдеры** в блоке **Проверка рабочего места**.
4. Откроется окно со списком провайдеров.
5. Выберите **КриптоПро CSP**.



6. В открывшемся окне активируйте настройку **Проверять флаг keyAgreement**.



Открыть статью на сайте

Активация лицензии КриптоАРМ

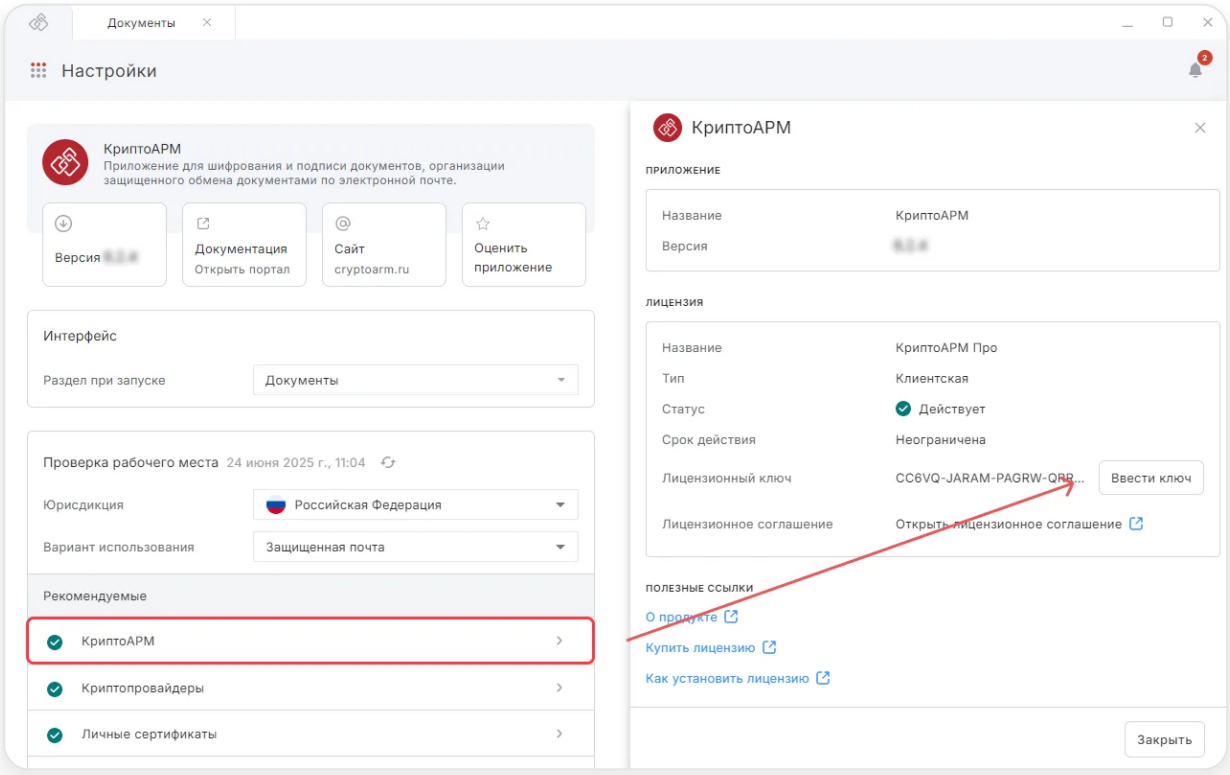
- Активация лицензии
- Проверка статуса лицензии

Активация лицензии

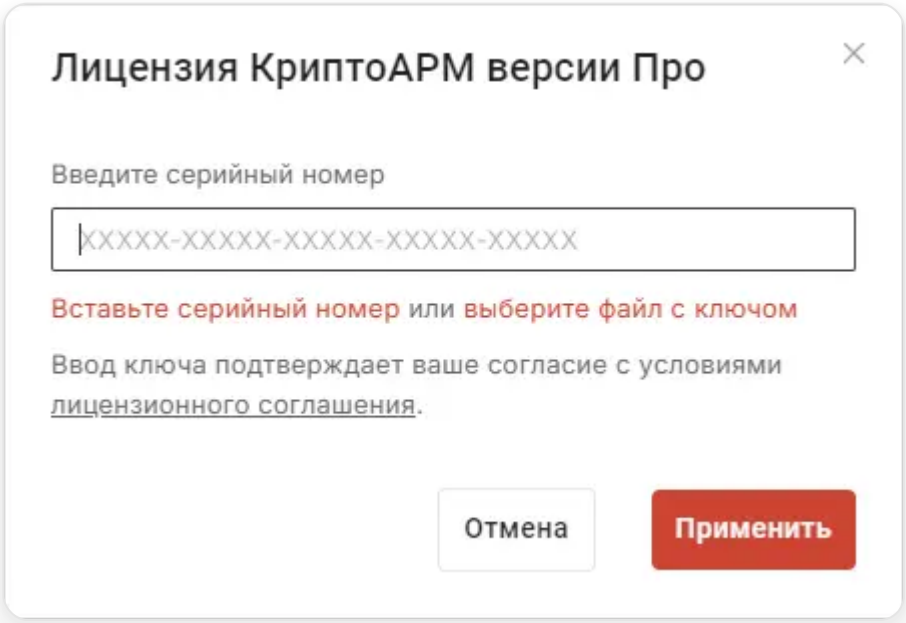
> ⚠️ **Примечание**: Приложение принимает лицензию, введённую без символа «-». Это удобно, если копируете лицензию из письма или документа, где дефисы отсутствуют.

Чтобы ввести ключ:

1. Перейдите в раздел **Настройки**.
2. Нажмите на панель **КриптоАРМ** в блоке **Проверка рабочего места**.
3. Откроется окно **КриптоАРМ** со сведениями о лицензии.

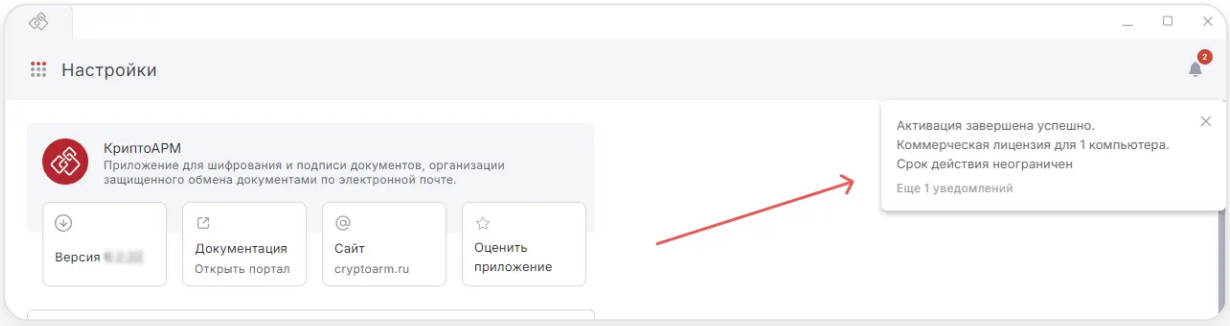


4. Нажмите на кнопку **Ввести ключ**.
5. Вставьте скопированный ключ из буфера или укажите путь к файлу с ним.



6. Нажмите **Применить**.

   Дождитесь окончания активации лицензии.



Если активация лицензии прошла успешно, её статус будет обновлён автоматически.

Проверка статуса лицензии

1. Перейдите на вкладку **Настройки**.
2. Выберите вариант использования **Защищенная почта** и запустите повторную проверку.
3. Нажмите на панель **КриптоАРМ**.
4. Откроется окно со сведениями о лицензии.

   Возможные статусы лицензии

Статус	Значение	Действия
✅ Действует	Лицензия действительна	Лицензия активна, все функции доступны.
⚠️ Отсутствует	Лицензия отсутствует или истекла	Введите новый ключ

Открыть статью на сайте

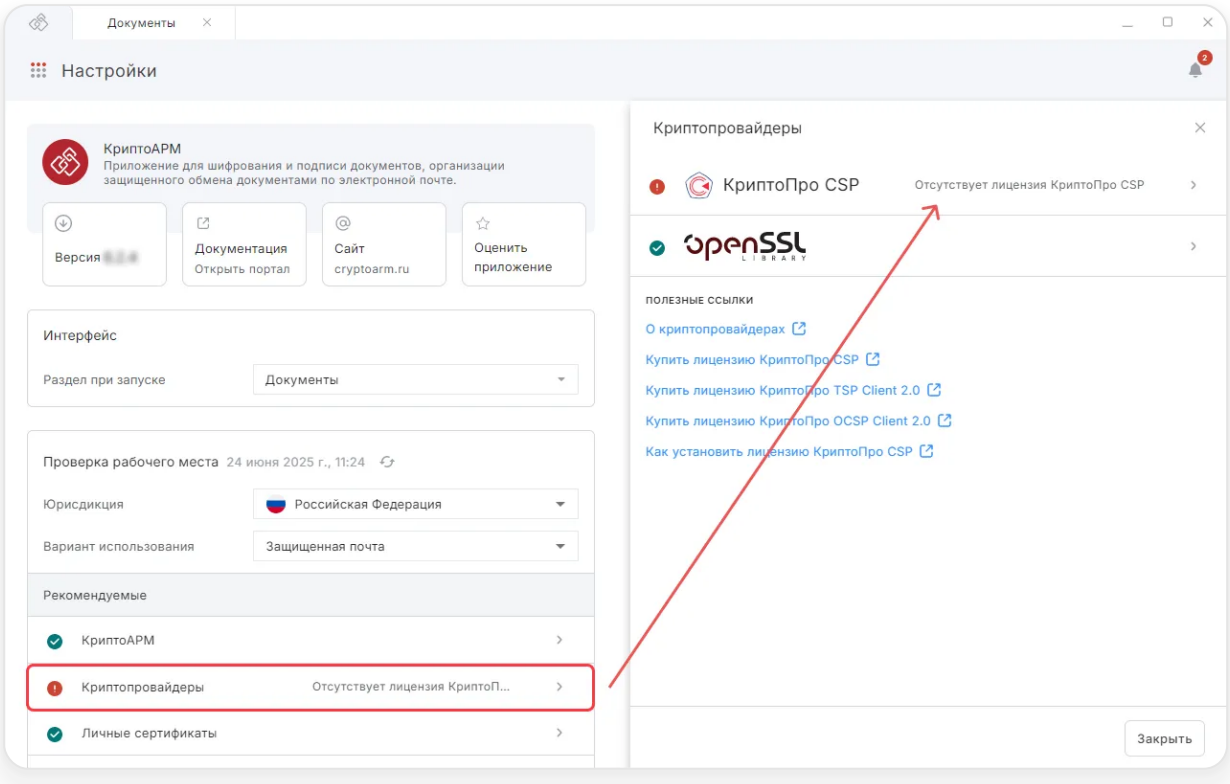
Активация лицензии КриптоПро CSP

- Активация лицензии
- Проверка статуса лицензии

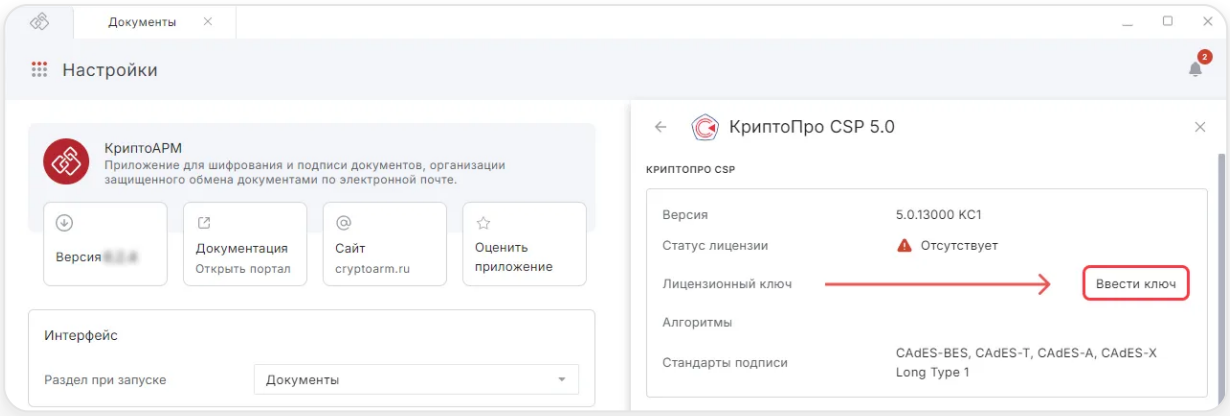
Активация лицензии

Для ввода лицензионного ключа выполните следующие шаги:

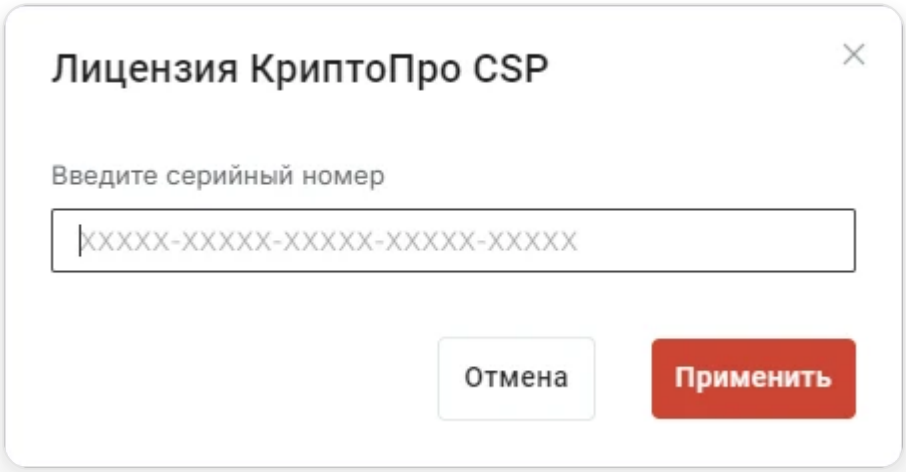
1. Перейдите в раздел **Настройки**.
2. При необходимости запустите проверку для юрисдикции **Российская Федерация**.
3. Нажмите на панель **Криптопровайдеры** в блоке **Проверка рабочего места**.
4. Откроется окно со списком провайдеров.
5. Выберите **КриптоПро CSP**.



6. В открывшемся окне нажмите на кнопку **Ввести ключ** в блоке **КриптоПро CSP**.



7. В открывшемся окне введите лицензионный ключ.



8. Нажмите **Применить**.

Дождитесь окончания активации лицензии.

Если активация лицензии прошла успешно, её статус будет обновлён автоматически.

Проверка статуса лицензии

1. Перейдите на вкладку **Настройки**.
2. Выберите вариант использования **Защищенная почта** и запустите повторную проверку.
3. Нажмите на панель **Криптопровайдеры**.
4. Откроется окно со списком провайдеров.
5. Выберите **КриптоПро CSP**.
6. Откроется окно со сведениями о лицензии:

   Возможные статусы лицензии

Статус	Значение	Действия
✅ Действует	Лицензия действительна	Лицензия активна, все функции доступны.
⚠️ Отсутствует	Лицензия отсутствует или истекла	Введите новый ключ

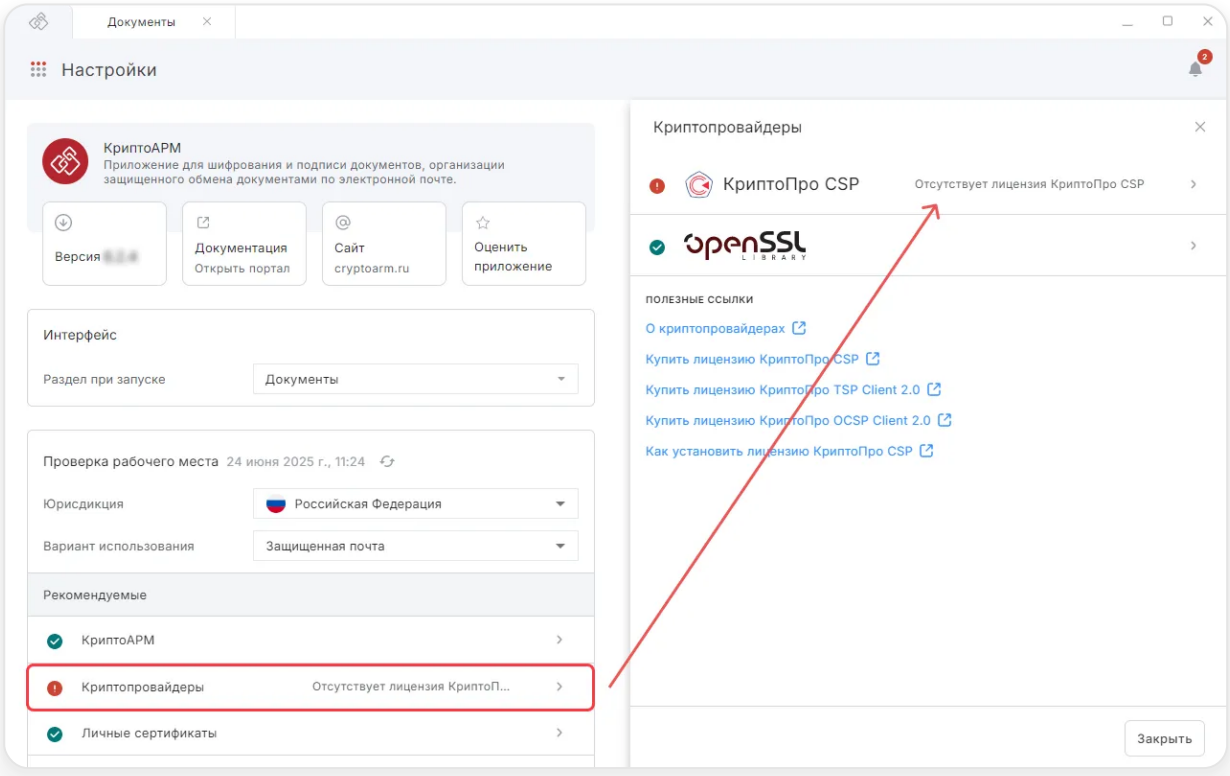
Открыть статью на сайте

Активация лицензии на модули TSP и OCSP

Ввод лицензии на модули TSP Client и OCSP Client выполняется аналогично установке лицензии на КриптоПро CSP.

Чтобы ввести лицензионный ключ на модули TSP Client и OCSP Client:

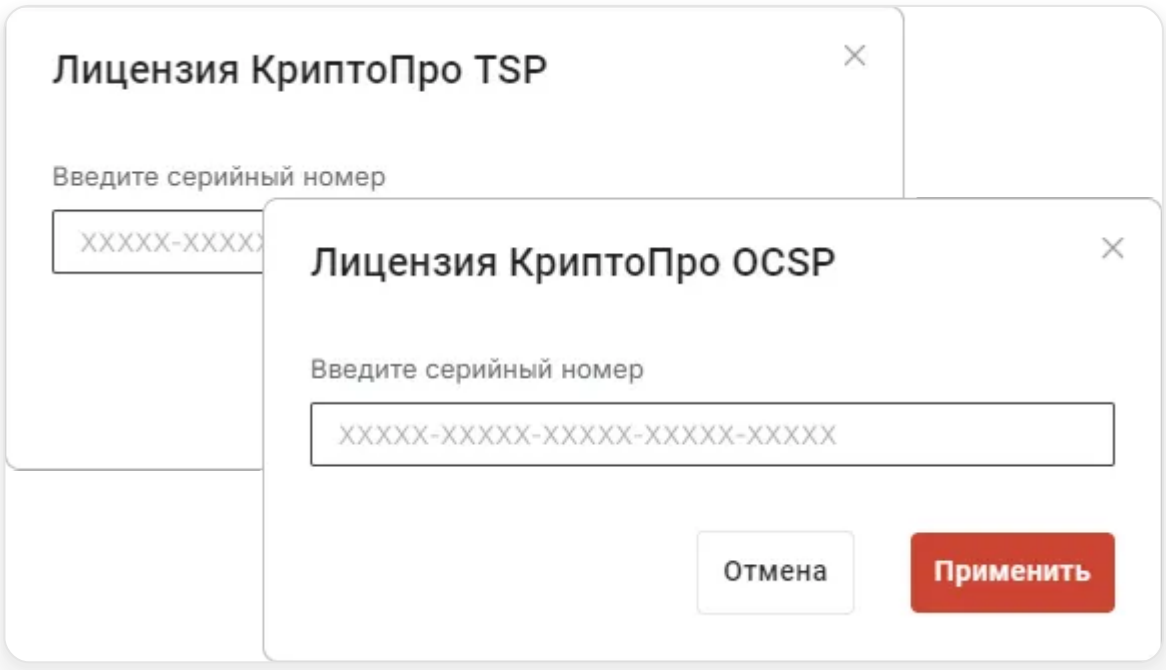
1. Перейдите в раздел **Настройки**.
2. При необходимости запустите проверку для юрисдикции **Российская Федерация**.
3. Нажмите на панель **Криптопровайдеры** в блоке **Проверка рабочего места**.
4. Откроется окно со списком провайдеров.
5. Выберите **КриптоПро CSP**.



6. Откроется окно со сведениями о лицензиях криптопровайдера КриптоПро CSP, модулей КриптоПро TSP Client и КриптоПро OCSP Client.
7. Нажмите на кнопку **Ввести ключ** в блоке **КриптоПро TSP Client** или **КриптоПро OCSP Client**.



8. В открывшемся окне введите лицензионный ключ.



9. Нажмите **Применить**.

Дождитесь окончания активации лицензии.

Открыть статью на сайте

Проверка рабочего места

- Основные понятия
- Запуск проверки
- Параметры проверки
- Системный отчет

Основные понятия

Проверка рабочего места — это удобный инструмент, который позволяет:

- Оценить готовность системы к работе с электронной подписью
- Выявить потенциальные проблемы в работе криптографических компонентов
- Проверить соответствие требованиям выбранного стандарта

Доступны две юрисдикции проверки:

- Российская Федерация (соответствие 63-ФЗ)
- Открытая криптография (международные стандарты)

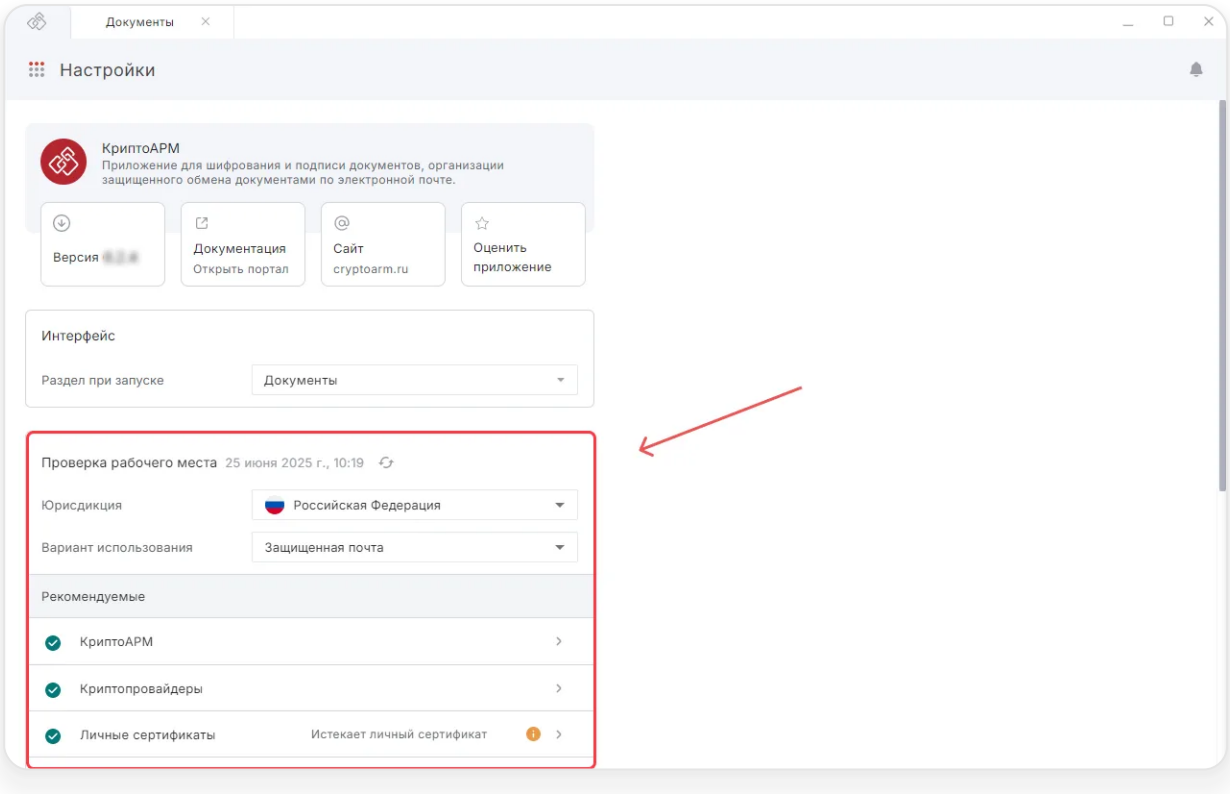
> ℹ️ Подробнее о параметрах проверки читайте в соответствующем разделе.

Запуск проверки

> 📌 Проверка запускается автоматически при открытии раздела **Настройки**. В любой момент доступен ручной запуск проверки.

Чтобы запустить проверку:

1. Перейдите на вкладку **Начальная страница**.
2. Выберите юрисдикцию.
3. Выберите подходящий вариант проверки.
4. Нажмите на кнопку **Обновить** .

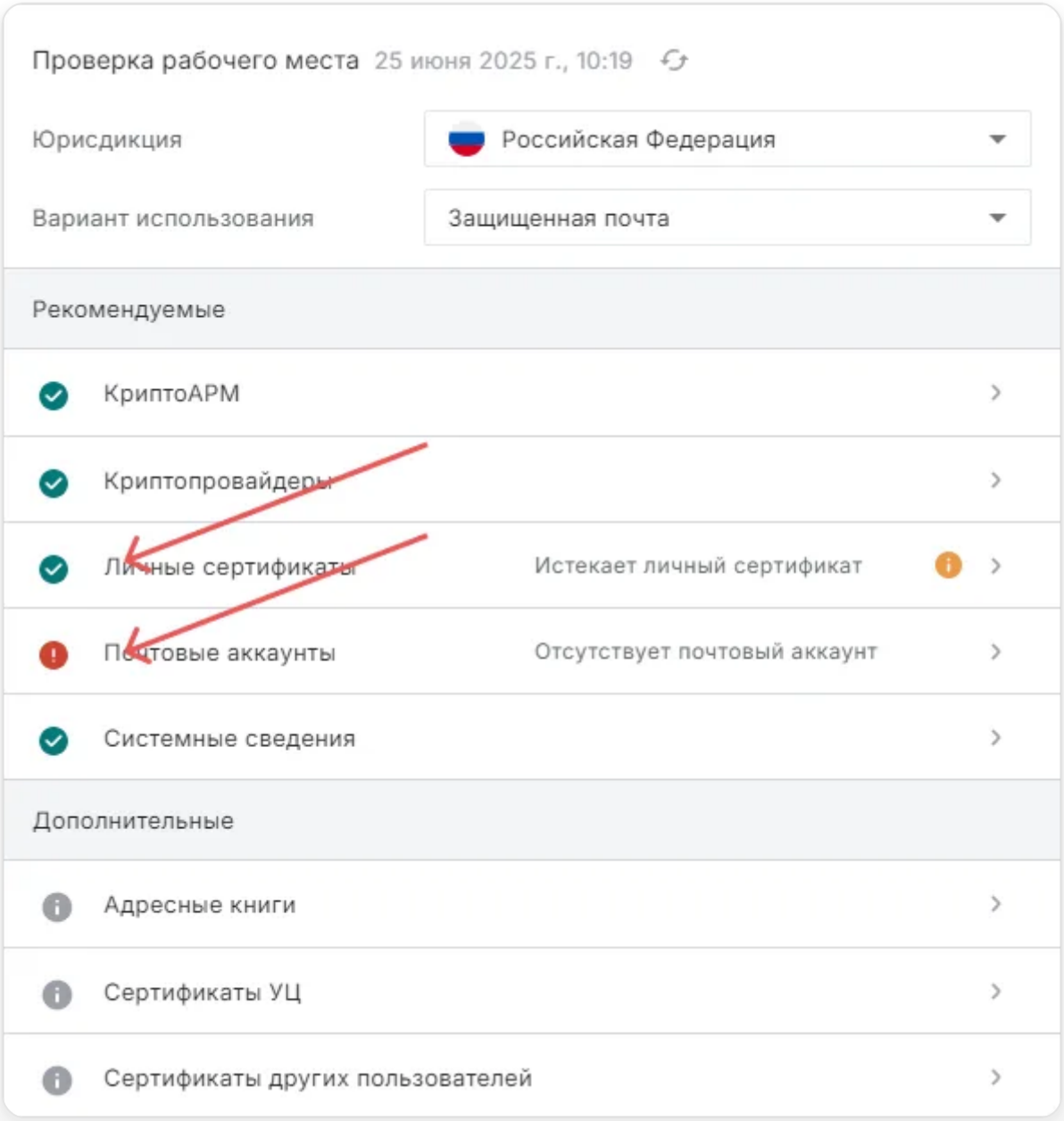


5. Дождитесь завершения проверки.

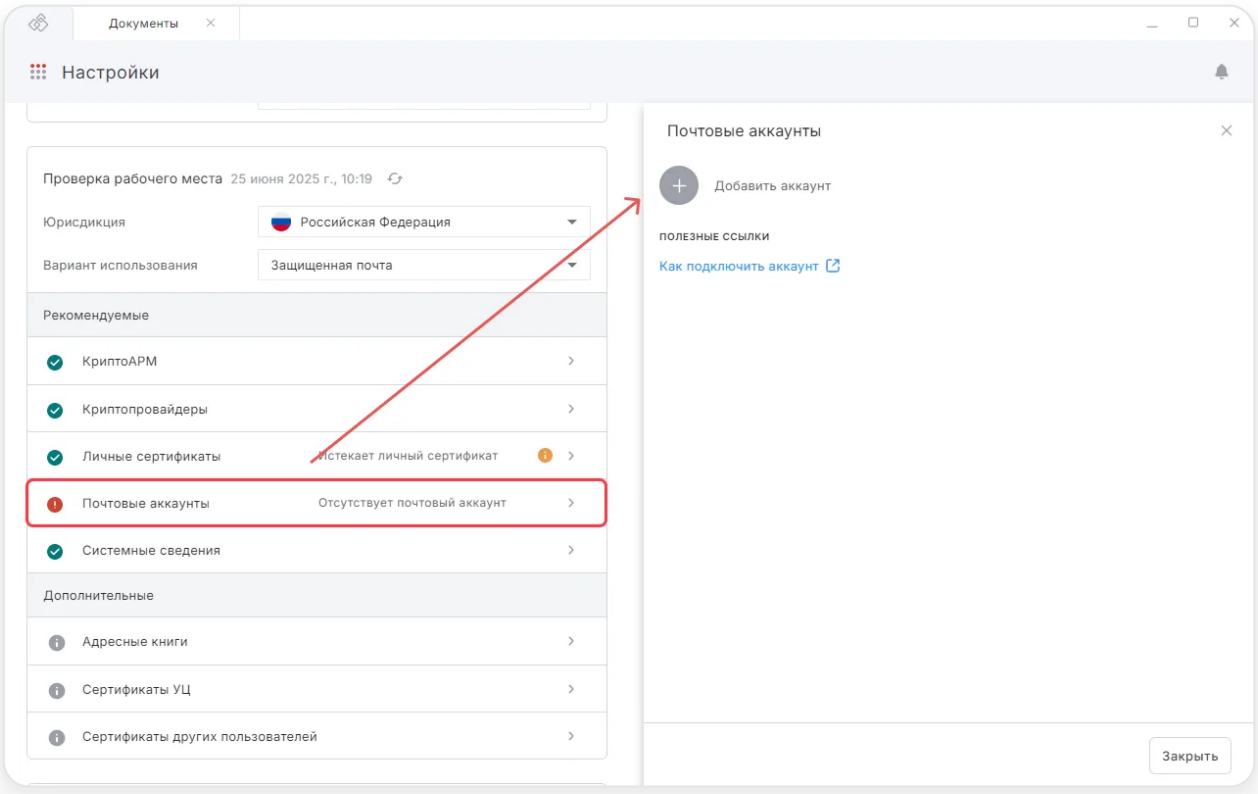
Анализ результатов

Для обязательных проверок будет отображен статус:

Статус	Иконка	Описание	Действия
Готово		Все компоненты работают корректно	Дополнительных действий не требуется
Ошибка		Обнаружены критические проблемы	Требуется устранение неполадок



Для просмотра деталей нажмите на соответствующую панель проверки.



В зависимости от выявленных проблем система предложит решения:

Криптографические компоненты:

- Установка КриптоПро CSP: Windows, Linux, macOS
- Активация лицензий: КриптоАРМ, КриптоПро CSP

Сертификаты:

- Установка личного сертификата: из ключевого контейнера, из файла .pfx, из DSS
- Создание самоподписанного сертификата
- Установка корневого или промежуточного сертификатов, сертификата другого пользователя

Почта и контакты:

- Добавление почтового аккаунта: Mail, Яндекс, Gmail, Outlook, iCloud, Rambler.
- Добавление контактов и адресных книг: Создание контакта, LDAP, ALDPro, CardDAV

Параметры проверки

Юрисдикции

Юрисдикция	Описание	Алгоритмы
Российская Федерация	Соответствие 63-ФЗ «Об электронной подписи»	Алгоритмы ГОСТ
Открытая криптография	Международные стандарты	RSA, ECDSA, DES, AES

Варианты использования

Вариант использования	Описание проверки	Проверяемые компоненты
Проверка подписи	Проверки для электронной подписи документов	1. Криптопровайдер для выбранной юрисдикции, 2. Соответствие системным требованиям
Подпись и шифрование	Проверки для создания электронной подписи и шифрования документов	1. Криптопровайдер для выбранной юрисдикции, 2. Соответствие системным требованиям, 3. Наличие действующего личного сертификата
Защищенная почта	Проверки для отправки подписанных и зашифрованных писем	1. Криптопровайдер для выбранной юрисдикции, 2. Соответствие системным требованиям, 3. Личный сертификат, 4. Почтовый аккаунт
Электронная почта	Проверки для отправки писем без подписи и шифрования	1. Соответствие системным требованиям, 2. Почтовый аккаунт

Системный отчет

Общая информация

Результаты проверки рабочего места можно сохранить в виде отчёта о системе. Этот отчёт может оказаться полезным, если возникнет необходимость обратиться в техническую поддержку.

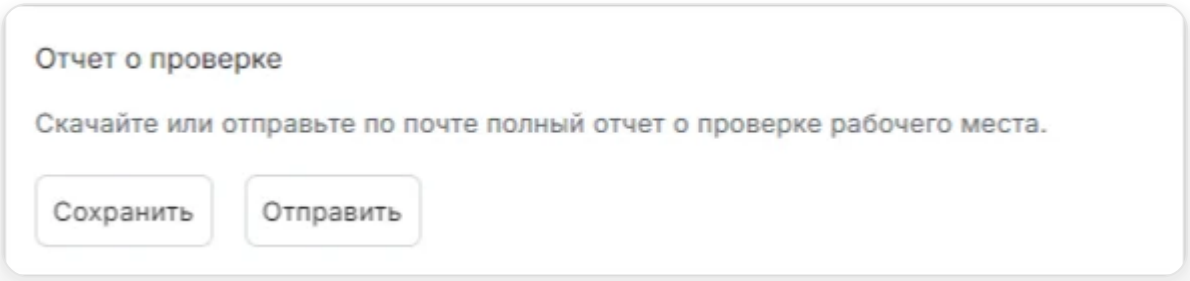
Отчёт можно сохранить в виде файла `.txt` или отправить по электронной почте прямо из приложения.

В файл будет записана следующая информация:

- сведения об операционной системе, процессоре и оперативной памяти;
- сведения о лицензии и версии приложения КриптоАРМ;
- сведения о криптопровайдере КриптоПро CSP и его лицензии;
- общее количество личных действительных сертификатов;
- общее количество контактов;
- сведения о почтовых аккаунтах (количество и протоколы).

Экспорт отчета

1. Перейдите на вкладку **Настройки**.
2. При необходимости запустите повторную проверку в блоке **Проверка рабочего места**.
3. Выберите одно из действий в блоке **Отчет о проверке**:
    - **Сохранить** - сохранение файла с отчетом на устройстве,
    - **Отправить** - отправка файла с отчетом из приложения.



⚠️ **Примечание**: Для отправки отчета по почте в приложении должен быть подключен почтовый аккаунт.

Открыть статью на сайте

С чего начать работу с почтой

Раздел **Почта** позволяет получать, читать и отправлять электронные письма, включая защищенные сообщения с использованием технологии S/MIME.

1. Проверка рабочего места

Проведите проверку рабочего места для варианта использования:

- **Защищенная почта** - для отправки подписанных и защифрованных писем,
- **Электронная почта** - для отправки писем без подписи и шифрования.

Если в ходе проверки будут обнаружены проблемы, устраните их.

2. Настройте почтовый аккаунт

- Добавление аккаунта
- Создание подписи в конце письма
- Создание правила сортировки писем
- Общие настройки

3. Создайте контакты или подключите адресные книги

- Создание контакта
- Импорт контакта из файла vCard
- Подключение адресной книги LDAP
- Подключение адресной книги ALD Pro
- Подключение адресной книги по протоколу CardDAV

4. Установите личный сертификат или создайте самоподписанный сертификат

- Установка сертификата из ключевого контейнера
- Установка сертификата из файла .pfx
- Установка сертификата из DSS
- Создание самоподписанного сертификата

5. Привяжите сертификаты

- Привязка сертификата подписи к аккаунту
- Привязка сертификата к контакту

Открыть статью на сайте

С чего начать работу с документами

1. Проверка рабочего места

Проведите проверку рабочего места для варианта использования:

- **Проверка подписи**,
- **Подпись и шифрование**.

Если в ходе проверки будут обнаружены проблемы, устраните их.

2. Установите личный сертификат или создайте самоподписанный сертификат

- Установка сертификата из ключевого контейнера
- Установка сертификата из файла .pfx
- Установка сертификата из DSS
- Создание самоподписанного сертификата

3. Настройте профиль подписи

- Создание профиля подписи

4. Создайте контакты или подключите адресные книги

- Создание контакта
- Импорт контакта из файла vCard
- Подключение адресной книги LDAP
- Подключение адресной книги ALD Pro
- Подключение адресной книги по протоколу CardDAV

5. Привяжите сертификаты к контактам

- Привязка сертификата к контакту

Теперь приложение готово к работе с электронной подписью!

Открыть статью на сайте

Добавление аккаунта

Приложение поддерживает работу с популярными почтовыми сервисами: Mail, Yandex, Gmail, Tegu, iCloud, Communigate Pro и Exchange.

Как подключить почтовый аккаунт

Шаг 1. Настройки подключения

1. Откройте форму добавления аккаунта:
   - Перейдите в раздел **Почта** и нажмите на кнопку **Добавить аккаунт** в центре окна (если аккаунты еще не подключены) или в окне со списком почтовых аккаунтов.
   - Перейдите в раздел **Настройки** → проверка **Почтовые аккаунты** и нажмите на кнопку **Добавить аккаунт**.
2. Укажите параметры подключения:
   - **Учетные данные**: адрес электронной почты и пароль,

     Используйте либо основной пароль от ящика, либо специальный пароль приложения, который необходимо создать в настройках почтового сервиса.

     Инструкции по созданию паролей приложений:

Почтовый сервис	Ссылка на инструкцию
Mail.ru	🔗 help.mail.ru
Yandex	🔗 yandex.ru/support
Gmail (Google)	🔗 support.google.com
Outlook.com (Microsoft)	🔗 support.microsoft.com

   - **Почтовый сервис**,
   - **Протокол подключения**,
   - **Адреса серверов** входящей и исходящей почты, параметры шифрования,

     > 💡 Для популярных почтовых сервисов настройки подставляются автоматически.

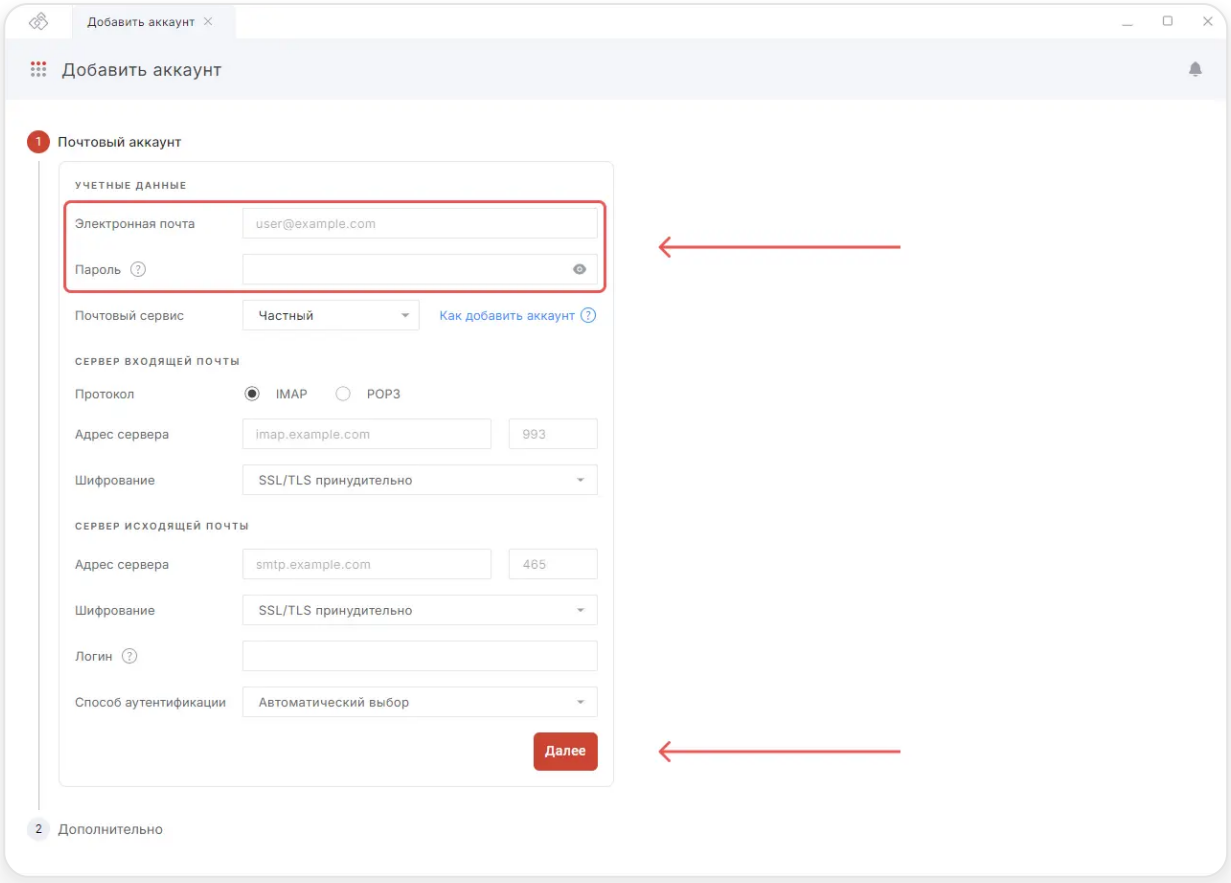
   - **Логин**,

Для некоторых почтовых серверов требуется обязательное наличие логина для отправки писем. Логин может совпадать с адресом почты или являться его первой частью до знака @

- **Способ аутентификации**.

  Выберите, каким образом приложение будет выполнять вход на почтовый сервер:

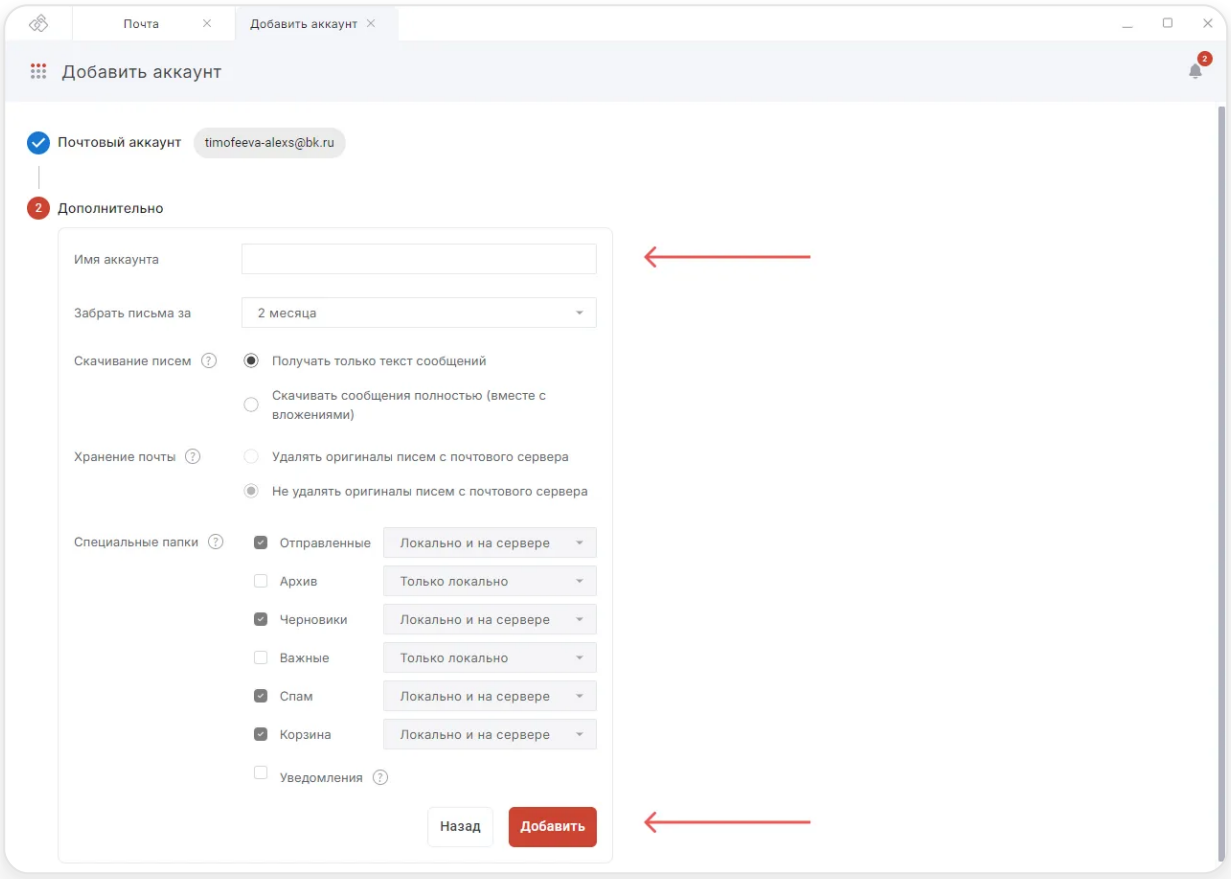
Способ	Для кого подходит	Особенности
Автоматический	Всем пользователям	Приложение само выбирает оптимальный вариант (рекомендуется)
Логин	Публичные почтовые сервисы (Gmail, Mail.ru, Яндекс и др.)	Имя пользователя и пароль передаются только по защищённому каналу
NTLM	Корпоративная почта Microsoft	Авторизация через доменную учётную запись (AD)
GSS-API (Kerberos)	Организации с доменной инфраструктурой	Вход без передачи пароля, используется Kerberos-билет



3. Нажмите на кнопку **Далее**.

Шаг 2. Настройки почтового ящика

1. Укажите **имя аккаунта** для отображения в приложении.
2. Настройте период, за который необходимо загрузить письма с сервера.
3. Укажите параметры загрузки писем:
   - **Получать только текст сообщений** — ускоренная загрузка без вложений. Загрузка вложений будет запущена при открытии письма.
   - **Скачивать сообщения полностью** (вместе с вложениями) — загрузка писем со всеми вложениями.
4. Укажите настройки хранения почты:
   - **Удалять оригиналы писем с почтового сервера** — письма будут удалены с почтового сервера после загрузки на устройство.
   - **Не удалять оригиналы писем с почтового сервера** — - письма останутся на сервере после загрузки на устройство.
5. При необходимости настройте специальные папки.
6. Нажмите **Добавить** для завершения.



После успешного добавления начнется синхронизация почты, которая может занять некоторое время в зависимости от объема писем.

> 💡 Для просмотра писем нового аккаунта сделайте его активным. Подробнее в инструкции Выбор активного аккаунта.

Возможные ошибки

При возникновении ошибок вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Решение
Ошибка соединения	Проверьте интернет-подключение и доступность почтового сервера
Ошибка подключения	Убедитесь в правильности: - Адреса электронной почты и пароля - Серверных настроек - Параметров подключения

Инструкции по теме

- Настройки аккаунта для отправки подписанных и зашифрованных писем
- Действия с аккаунтами
- Как настроить сортировку писем
- Как создать подпись (текстовая подпись в конце письма)
- Общие настройки аккаунта

Открыть статью на сайте

Добавление аккаунта mail.ru

- Как подключить почтовый аккаунт
- Возможные ошибки

Как подключить почтовый аккаунт

Шаг 1. Создание пароля приложения

В качестве пароля от почтового ящика выступает специальный пароль приложения, который необходимо создать в настройках почтового сервиса.

> 🔍 Подробнее о создании пароля приложения читайте на портале официальной документации help.mail.ru.

Шаг 2. Настройки подключения

1. Откройте форму добавления аккаунта:
   - Перейдите в раздел **Почта** и нажмите на кнопку **Добавить аккаунт** в центре окна (если аккаунты еще не подключены) или в окне со списком почтовых аккаунтов.
   - Перейдите в раздел **Настройки** → проверка **Почтовые аккаунты** и нажмите на кнопку **Добавить аккаунт**.
2. Укажите параметры подключения:
   - **Учетные данные**: адрес электронной почты и пароль, созданный на шаге 1,
   - **Почтовый сервис**: mail.ru,

     > 💡 Для популярных сервисов настройки подставляются автоматически.

   - **Протокол подключения**,
   - **Адреса серверов** входящей и исходящей почты, параметры шифрования.

     > 💡 Настройки сервера входящей и исходящей почты будут поставлены автоматически. Если этого не произойдет, заполните их самостоятельно. Ссылка на настройки Mail.ru.

- **Способ аутентификации**: автоматический или логин.

3. Нажмите на кнопку **Далее**.

Шаг 2. Настройки почтового ящика

1. Укажите имя аккаунта для отображения в приложении.
2. Настройте период, за который необходимо загрузить письма с сервера.
3. Укажите параметры загрузки писем:
   - **Получать только текст сообщений** — ускоренная загрузка без вложений. Загрузка вложений будет запущена при открытии письма.
   - **Скачивать сообщения полностью** (вместе с вложениями) — загрузка писем со всеми вложениями.
4. Укажите настройки хранения почты:
   - **Удалять оригиналы писем с почтового сервера** — письма будут удалены с почтового сервера после загрузки на устройство.
   - **Не удалять оригиналы писем с почтового сервера** — - письма останутся на сервере после загрузки на устройство.
5. При необходимости настройте специальные папки.
6. Нажмите **Добавить** для завершения.

После успешного добавления начнется синхронизация почты, которая может занять некоторое время в зависимости от объема писем.

> 💡 Для просмотра писем нового аккаунта сделайте его активным. Подробнее в инструкции Выбор активного аккаунта.

Возможные ошибки

При возникновении ошибок вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Решение
Ошибка соединения	Проверьте интернет-подключение и доступность почтового сервера
Ошибка подключения	

Ошибка	Решение
	Убедитесь в правильности: - Адреса электронной почты и пароля - Серверных настроек - Параметров подключения

Инструкции по теме

- Настройки аккаунта для отправки подписанных и зашифрованных писем
- Действия с аккаунтами
- Настройка сортировки писем
- Создание подписи (текстовая подпись в конце письма)
- Общие настройки аккаунта

Открыть статью на сайте

Добавление аккаунта yandex.ru

- Как подключить почтовый аккаунт
- Возможные ошибки

Как подключить почтовый аккаунт

Шаг 1. Настройки в Яндекс Почте

1. Откройте раздел **Почтовые программы** в настройках **Яндекс Почты**.
2. Выберите опции **Разрешить доступ к почтовому ящику с помощью почтовых клиентов** → **С сервера imap.yandex.ru по протоколу IMAP** и **Пароли приложений и OAuth-токены**.
3. Сохраните изменения.

Шаг 2. Создание пароля приложения

В качестве пароля от почтового ящика выступает специальный пароль приложения, который необходимо создать в настройках почтового сервиса.

> 🔍 Подробнее о создании пароля приложения читайте на портале официальной документации yandex.ru.

Шаг 3. Настройки подключения

1. Откройте форму добавления аккаунта:
    - Перейдите в раздел **Почта** и нажмите на кнопку **Добавить аккаунт** в центре окна (если аккаунты еще не подключены) или в окне со списком почтовых аккаунтов.
    - Перейдите в раздел **Настройки** → проверка **Почтовые аккаунты** и нажмите на кнопку **Добавить аккаунт**.
2. Укажите параметры подключения:
    - **Учетные данные**: адрес электронной почты и пароль, созданный на шаге 2,
    - **Почтовый сервис**: yandex.ru,

      > 💡 Для популярных сервисов настройки подставляются автоматически.

    - **Протокол подключения**,

- **Адреса серверов** входящей и исходящей почты, параметры шифрования.

> 💡 Настройки сервера входящей и исходящей почты будут поставлены автоматически. Если этого не произойдет, заполните их самостоятельно. Ссылка на настройки Яндекс.

- **Способ аутентификации**: автоматический или логин.

3. Нажмите на кнопку **Далее**.

Шаг 4. Настройки почтового ящика

1. Укажите имя аккаунта для отображения в приложении.
2. Настройте период, за который необходимо загрузить письма с сервера.
3. Укажите параметры загрузки писем:
   - **Получать только текст сообщений** — ускоренная загрузка без вложений. Загрузка вложений будет запущена при открытии письма.
   - **Скачивать сообщения полностью** (вместе с вложениями) — загрузка писем со всеми вложениями.
4. Укажите настройки хранения почты:
   - **Удалять оригиналы писем с почтового сервера** — письма будут удалены с почтового сервера после загрузки на устройство.
   - **Не удалять оригиналы писем с почтового сервера** — - письма останутся на сервере после загрузки на устройство.
5. При необходимости настройте специальные папки.
6. Нажмите **Добавить** для завершения.

После успешного добавления начнется синхронизация почты, которая может занять некоторое время в зависимости от объема писем.

> 💡 Для просмотра писем нового аккаунта сделайте его активным. Подробнее в инструкции Выбор активного аккаунта.

Возможные ошибки

При возникновении ошибок вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Решение
Ошибка соединения	Проверьте интернет-подключение и доступность почтового сервера
Ошибка подключения	Убедитесь в правильности: - Адреса электронной почты и пароля - Серверных настроек - Параметров подключения

Инструкции по теме

- Настройки аккаунта для отправки подписанных и зашифрованных писем
- Действия с аккаунтами
- Настройка сортировки писем
- Создание подписи (текстовая подпись в конце письма)
- Общие настройки аккаунта

Открыть статью на сайте

Добавление аккаунта gmail.com

- Как подключить почтовый аккаунт
- Возможные ошибки

Как подключить почтовый аккаунт

Шаг 1. Создание пароля приложения

В качестве пароля от почтового ящика выступает специальный пароль приложения, который необходимо создать в настройках почтового сервиса.

> 🔍 Подробнее о создании пароля приложения читайте на портале официальной документации support.google.com.

Шаг 2. Настройки подключения

1. Откройте форму добавления аккаунта:
   - Перейдите в раздел **Почта** и нажмите на кнопку **Добавить аккаунт** в центре окна (если аккаунты еще не подключены) или в окне со списком почтовых аккаунтов.
   - Перейдите в раздел **Настройки** → проверка **Почтовые аккаунты** и нажмите на кнопку **Добавить аккаунт**.
2. Укажите параметры подключения:
   - **Учетные данные**: адрес электронной почты и пароль, созданный на шаге 1,
   - **Почтовый сервис**: gmail.com,

     > 💡 Для популярных сервисов настройки подставляются автоматически.

   - **Протокол подключения**,
   - **Адреса серверов** входящей и исходящей почты, параметры шифрования.

     > 💡 Настройки сервера входящей и исходящей почты будут поставлены автоматически. Если этого не произойдет, заполните их самостоятельно. Ссылка на настройки Gmail.

- **Способ аутентификации**: автоматический или логин.

3. Нажмите на кнопку **Далее**.

Шаг 3. Настройки почтового ящика

1. Укажите имя аккаунта для отображения в приложении.
2. Настройте период, за который необходимо загрузить письма с сервера.
3. Укажите параметры загрузки писем:
   - **Получать только текст сообщений** — ускоренная загрузка без вложений. Загрузка вложений будет запущена при открытии письма.
   - **Скачивать сообщения полностью** (вместе с вложениями) — загрузка писем со всеми вложениями.
4. Укажите настройки хранения почты:
   - **Удалять оригиналы писем с почтового сервера** — письма будут удалены с почтового сервера после загрузки на устройство.
   - **Не удалять оригиналы писем с почтового сервера** — - письма останутся на сервере после загрузки на устройство.
5. При необходимости настройте специальные папки.
6. Нажмите **Добавить** для завершения.

После успешного добавления начнется синхронизация почты, которая может занять некоторое время в зависимости от объема писем.

> 💡 Для просмотра писем нового аккаунта сделайте его активным. Подробнее в инструкции Выбор активного аккаунта.

Возможные ошибки

При возникновении ошибок вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Решение
Ошибка соединения	Проверьте интернет-подключение и доступность почтового сервера
Ошибка подключения	

Ошибка	Решение
	Убедитесь в правильности: - Адреса электронной почты и пароля - Серверных настроек - Параметров подключения

Инструкции по теме

- Настройки аккаунта для отправки подписанных и зашифрованных писем
- Действия с аккаунтами
- Настройка сортировки писем
- Создание подписи (текстовая подпись в конце письма)
- Общие настройки аккаунта

Открыть статью на сайте

Добавление аккаунта outlook.com

- Как подключить почтовый аккаунт
- Возможные ошибки

Как подключить почтовый аккаунт

Шаг 1. Создание пароля приложения

В качестве пароля от почтового ящика выступает специальный пароль приложения, который необходимо создать в настройках почтового сервиса.

> 🔍 Подробнее о создании пароля приложения читайте на портале официальной документации support.microsoft.com.

Шаг 2. Настройки подключения

1. Откройте форму добавления аккаунта:
   - Перейдите в раздел **Почта** и нажмите на кнопку **Добавить аккаунт** в центре окна (если аккаунты еще не подключены) или в окне со списком почтовых аккаунтов.
   - Перейдите в раздел **Настройки** → проверка **Почтовые аккаунты** и нажмите на кнопку **Добавить аккаунт**.
2. Укажите параметры подключения:
   - **Учетные данные**: адрес электронной почты и пароль, созданный на шаге 1,
   - **Почтовый сервис**: outlook.com,

     > 💡 Для популярных сервисов настройки подставляются автоматически.

   - **Протокол подключения**,
   - **Адреса серверов** входящей и исходящей почты, параметры шифрования.

     > 💡 Настройки сервера входящей и исходящей почты будут поставлены автоматически. Если этого не произойдет, заполните их самостоятельно. Ссылка на настройки Outlook.

- **Способ аутентификации**: автоматический или логин.

3. Нажмите на кнопку **Далее**.

Шаг 3. Настройки почтового ящика

1. Укажите имя аккаунта для отображения в приложении.
2. Настройте период, за который необходимо загрузить письма с сервера.
3. Укажите параметры загрузки писем:
   - **Получать только текст сообщений** — ускоренная загрузка без вложений. Загрузка вложений будет запущена при открытии письма.
   - **Скачивать сообщения полностью** (вместе с вложениями) — загрузка писем со всеми вложениями.
4. Укажите настройки хранения почты:
   - **Удалять оригиналы писем с почтового сервера** — письма будут удалены с почтового сервера после загрузки на устройство.
   - **Не удалять оригиналы писем с почтового сервера** — - письма останутся на сервере после загрузки на устройство.
5. При необходимости настройте специальные папки.
6. Нажмите **Добавить** для завершения.

После успешного добавления начнется синхронизация почты, которая может занять некоторое время в зависимости от объема писем.

> 💡 Для просмотра писем нового аккаунта сделайте его активным. Подробнее в инструкции Выбор активного аккаунта.

Возможные ошибки

При возникновении ошибок вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Решение
Ошибка соединения	Проверьте интернет-подключение и доступность почтового сервера
Ошибка подключения	

Ошибка	Решение
	Убедитесь в правильности: - Адреса электронной почты и пароля - Серверных настроек - Параметров подключения

Инструкции по теме

- Настройки аккаунта для отправки подписанных и зашифрованных писем
- Действия с аккаунтами
- Настройка сортировки писем
- Создание подписи (текстовая подпись в конце письма)
- Общие настройки аккаунта

Открыть статью на сайте

Добавление аккаунта icloud.com

Как подключить почтовый аккаунт

Шаг 1. Создание пароля приложения

В качестве пароля от почтового ящика выступает специальный пароль приложения, который необходимо создать в настройках почтового сервиса.

> 🔍 Подробнее о создании пароля приложения читайте на портале официальной документации support.apple.com.

Шаг 2. Настройки подключения

1. Откройте форму добавления аккаунта:
   - Перейдите в раздел **Почта** и нажмите на кнопку **Добавить аккаунт** в центре окна (если аккаунты еще не подключены) или в окне со списком почтовых аккаунтов.
   - Перейдите в раздел **Настройки** → проверка **Почтовые аккаунты** и нажмите на кнопку **Добавить аккаунт**.
2. Укажите параметры подключения:
   - **Учетные данные**: адрес электронной почты и пароль, созданный на шаге 1,
   - **Почтовый сервис**: icloud.com,

     > 💡 Для популярных сервисов настройки подставляются автоматически.

   - **Протокол подключения**,
   - **Адреса серверов** входящей и исходящей почты, параметры шифрования.

     > 💡 Настройки сервера входящей и исходящей почты будут поставлены автоматически. Если этого не произойдет, заполните их самостоятельно. Ссылка на настройки ICloud.

   - **Способ аутентификации**: автоматический или логин.
3. Нажмите на кнопку **Далее**.

Шаг 3. Настройки почтового ящика

1. Укажите имя аккаунта для отображения в приложении.
2. Настройте период, за который необходимо загрузить письма с сервера.
3. Укажите параметры загрузки писем:
   - **Получать только текст сообщений** — ускоренная загрузка без вложений. Загрузка вложений будет запущена при открытии письма.
   - **Скачивать сообщения полностью** (вместе с вложениями) — загрузка писем со всеми вложениями.
4. Укажите настройки хранения почты:
   - **Удалять оригиналы писем с почтового сервера** — письма будут удалены с почтового сервера после загрузки на устройство.
   - **Не удалять оригиналы писем с почтового сервера** — - письма останутся на сервере после загрузки на устройство.
5. При необходимости настройте специальные папки.
6. Нажмите **Добавить** для завершения.

После успешного добавления начнется синхронизация почты, которая может занять некоторое время в зависимости от объема писем.

> 💡 Для просмотра писем нового аккаунта сделайте его активным. Подробнее в инструкции Выбор активного аккаунта.

Возможные ошибки

При возникновении ошибок вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Решение
Ошибка соединения	Проверьте интернет-подключение и доступность почтового сервера
Ошибка подключения	Убедитесь в правильности: - Адреса электронной почты и пароля - Серверных настроек - Параметров подключения

Инструкции по теме

- Настройки аккаунта для отправки подписанных и зашифрованных писем
- Действия с аккаунтами
- Настройка сортировки писем
- Создание подписи (текстовая подпись в конце письма)
- Общие настройки аккаунта

Открыть статью на сайте

Добавление аккаунта rambler.ru

- Как подключить почтовый аккаунт
- Возможные ошибки

Как подключить почтовый аккаунт

Шаг 1. Настройки в сервисе Rambler

Для работы с письмами через почтовый клиент включите **Доступ к почтовому ящику с помощью почтовых клиентов**.

> 🔍 Подробнее о настройке читайте на портале официальной документации help.rambler.ru.

Шаг 2. Создание пароля приложения

В качестве пароля от почтового ящика выступает специальный пароль приложения, который необходимо создать в настройках почтового сервиса. Подробнее о создании пароля приложения читайте на портале официальной документации help.rambler.ru.

Шаг 3. Настройки подключения

1. Откройте форму добавления аккаунта:
    - Перейдите в раздел **Почта** и нажмите на кнопку **Добавить аккаунт** в центре окна (если аккаунты еще не подключены) или в окне со списком почтовых аккаунтов.
    - Перейдите в раздел **Настройки** → проверка **Почтовые аккаунты** и нажмите на кнопку **Добавить аккаунт**.
2. Укажите параметры подключения:
    - **Учетные данные**: адрес электронной почты и пароль, созданный на шаге 1,
    - **Почтовый сервис**: rambler.ru,

      > 💡 Для популярных сервисов настройки подставляются автоматически.

    - **Протокол подключения**,
    - **Адреса серверов** входящей и исходящей почты, параметры шифрования.

> 💡 Настройки сервера входящей и исходящей почты будут поставлены автоматически. Если этого не произойдет, заполните их самостоятельно. Ссылка на настройки Rambler.

- **Способ аутентификации**: автоматический или логин.

3. Нажмите на кнопку **Далее**.

Шаг 4. Настройки почтового ящика

1. Укажите имя аккаунта для отображения в приложении.
2. Настройте период, за который необходимо загрузить письма с сервера.
3. Укажите параметры загрузки писем:
   - **Получать только текст сообщений** — ускоренная загрузка без вложений. Загрузка вложений будет запущена при открытии письма.
   - **Скачивать сообщения полностью** (вместе с вложениями) — загрузка писем со всеми вложениями.
4. Укажите настройки хранения почты:
   - **Удалять оригиналы писем с почтового сервера** — письма будут удалены с почтового сервера после загрузки на устройство.
   - **Не удалять оригиналы писем с почтового сервера** — - письма останутся на сервере после загрузки на устройство.
5. При необходимости настройте специальные папки.
6. Нажмите **Добавить** для завершения.

После успешного добавления начнется синхронизация почты, которая может занять некоторое время в зависимости от объема писем.

> 💡 Для просмотра писем нового аккаунта сделайте его активным. Подробнее в инструкции Выбор активного аккаунта.

Возможные ошибки

При возникновении ошибок вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Решение
Ошибка соединения	Проверьте интернет-подключение и доступность почтового сервера
Ошибка подключения	Убедитесь в правильности: - Адреса электронной почты и пароля - Серверных настроек - Параметров подключения

Инструкции по теме

- Настройки аккаунта для отправки подписанных и зашифрованных писем
- Действия с аккаунтами
- Настройка сортировки писем
- Создание подписи (текстовая подпись в конце письма)
- Общие настройки аккаунта

Открыть статью на сайте

Действия с аккаунтами

- Выбор активного аккаунта
- Изменение настроек почтового аккаунта
- Удаление почтового аккаунта

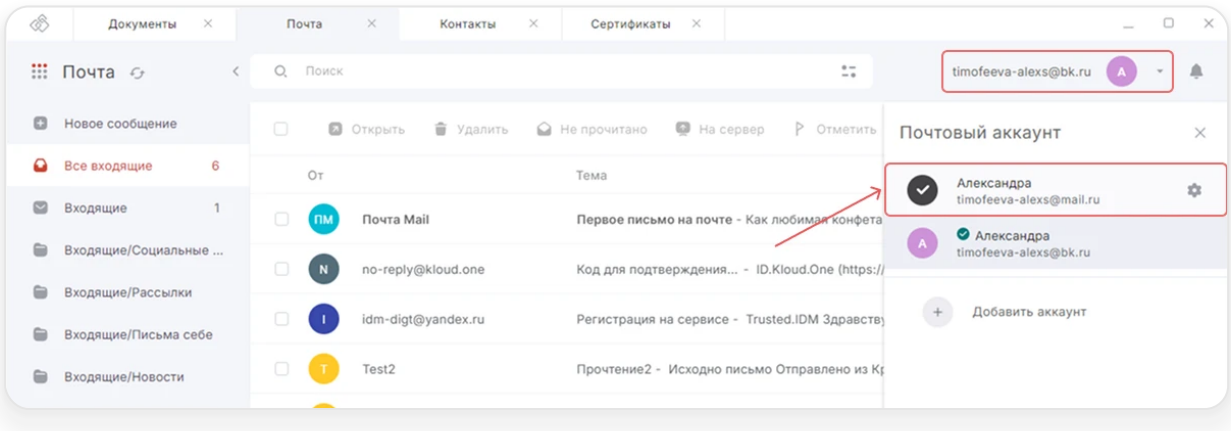
Выбор активного аккаунта

При работе с несколькими почтовыми аккаунтами:

- В папке **Все входящие** отображаются письма со всех аккаунтов,
- В остальных разделах показываются только письма активного аккаунта.

Как выбрать активный аккаунт

1. Перейдите в раздел **Почта**.
2. Откройте окно со списком почтовых аккаунтов, которое вызывается по клику на имя активного аккаунта.
3. Наведите курсор на аккаунт, который хотите сделать активным, и нажмите на его аватар.



Аккаунт отмечается иконкой и становится активным. В списке писем **Входящие** и вложенных папках отображаются письма добавленного аккаунта.

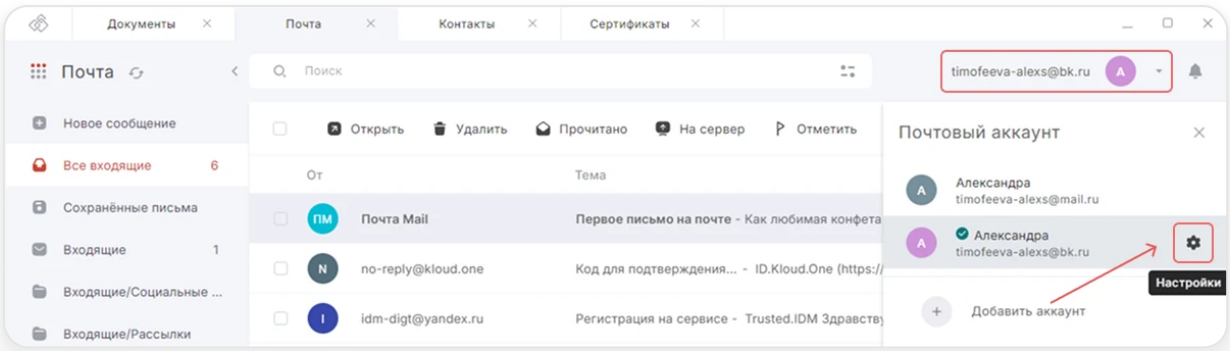
Изменение настроек почтового аккаунта

Чтобы открыть настройки почтового аккаунта:

1. Перейдите в раздел **Почта**.
2. Нажмите на имя активного аккаунта в верхнем правом углу окна.

3. Откроется окно со списком аккаунтов.

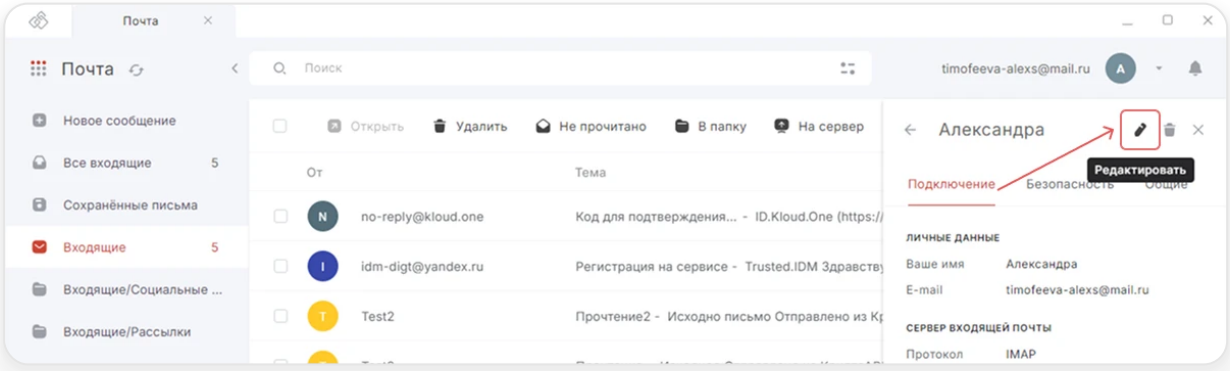
4. Наведите курсор на аккаунт, настройки которого надо изменить.



5. Нажмите всплывающую кнопку **Настройки**.

6. Откроется форма просмотра настроек аккаунта.

7. Нажмите кнопку **Редактировать** .



8. Откроется новая вкладка с настройками почтового аккаунта.

9. Внесите необходимые изменения на вкладках:

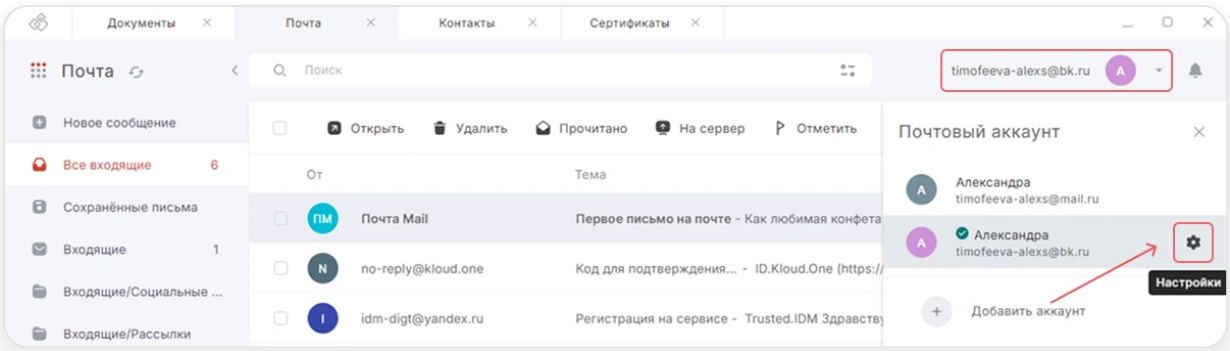
   - Настройки безопасности,
   - Настройки подключения,
   - Общие настройки,
   - Подписи.

Изменения сохраняются автоматически и не требуют дополнительного подтверждения.

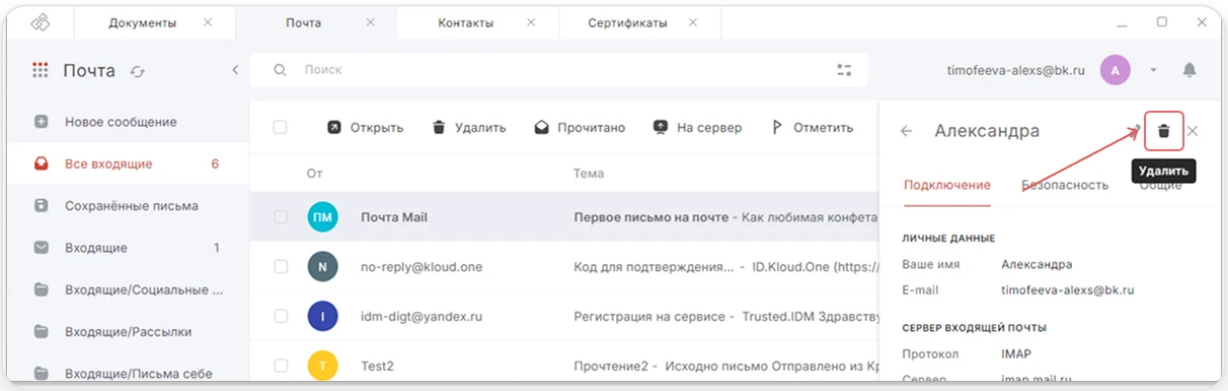
Удаление почтового аккаунта

Чтобы удалить почтовый аккаунт в приложении:

1. Перейдите в раздел **Почта**.
2. Откройте окно со списком почтовых аккаунтов, которое вызывается по клику на имя активного аккаунта.
3. В списке наведите курсор на почтовый аккаунт, который хотите удалить.



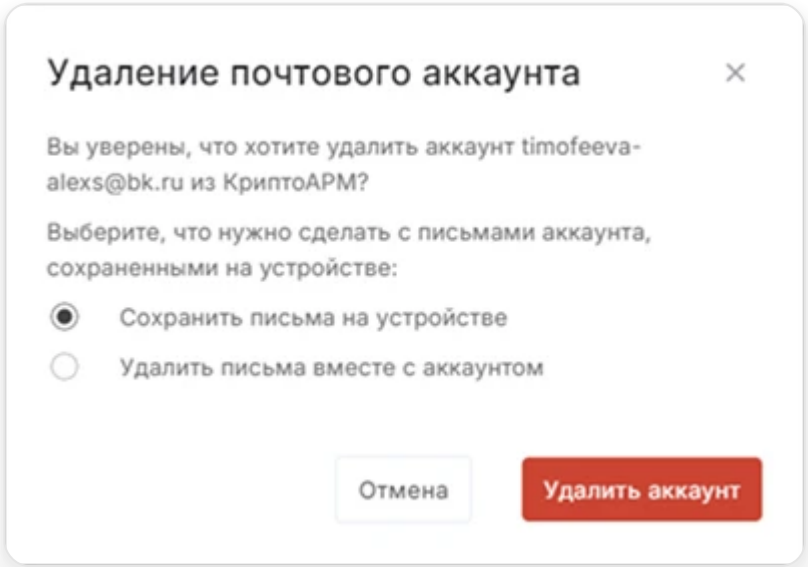
4. Нажмите всплывающую кнопку **Настройки**.
5. Откроется форма просмотра настроек аккаунта.
6. Нажмите кнопку **Удалить** .



7. Подтвердите удаление.

Если в вашем аккаунте имеются письма в папке **Сохраненные письма**, вам необходимо выбрать, как с ними поступить:

- **Удалить письма вместе с аккаунтом** — все письма будут безвозвратно удалены.
- **Сохранить письма на устройстве** — все письма из этого аккаунта сохранятся в папке **Сохраненные письма**, а сам аккаунт будет удален из списка подключенных.



Инструкции по теме

- Добавление почтового аккаунта
- Настройки аккаунта для отправки подписанных и зашифрованных писем
- Настройка сортировки писем
- Создание подписи (текстовая подпись в конце письма)
- Общие настройки аккаунта

Открыть статью на сайте

Настройки защищенной почты

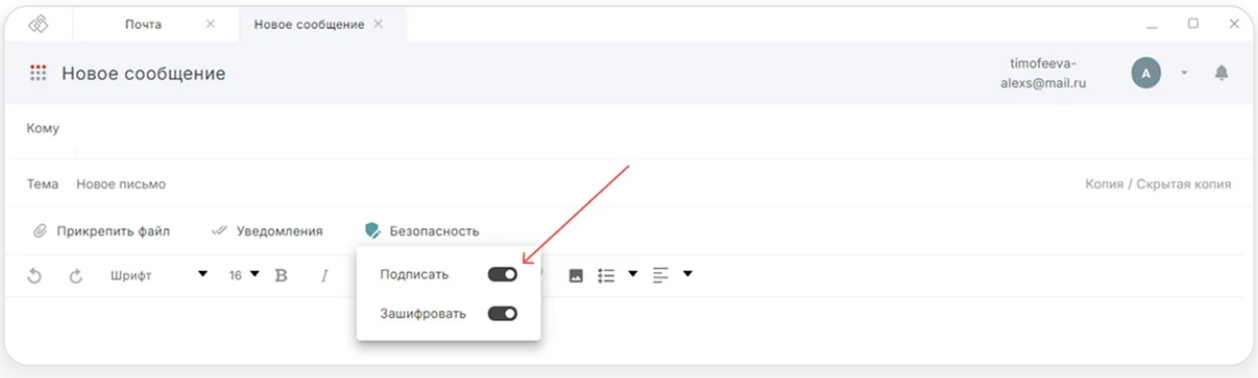
- Настройка подписи и шифрования писем
- Привязка сертификата подписи
- Отображение информации о сертификате
- Настройки шифрования
- Хранение зашифрованных сообщений
- Скачивание писем
- Хранение почты

Настройка подписи и шифрования писем

Чтобы активировать настройки подписи и шифрования исходящих писем:

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Безопасность**.
3. Активируйте переключатели в блоке **Безопасность почты**:
    - **Шифровать содержимое и вложения исходящих сообщений** - автоматическое шифрование писем в адрес получателей, имеющих привязанные сертификаты.
    - **Добавлять электронную подпись к исходящим сообщениям** - автоматическое добавление электронной подписи к исходящим письмам при условии, что к аккаунту привязан сертификат подписи.

При открытии вкладки с новым письмом переключатели будут выставлены в соответствии с указанными настройками.

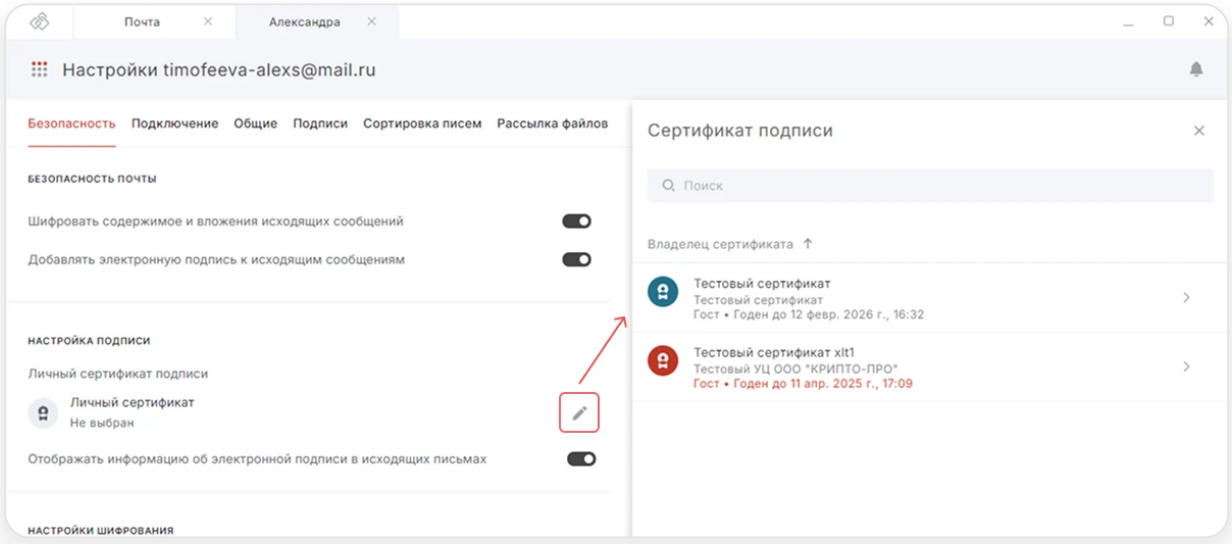


Привязка сертификата подписи

> 💡 В приложении к аккаунту можно привязать только один сертификат из хранилища «Личные сертификаты».

Чтобы привязать сертификат к почтовому аккаунту:

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Безопасность**.
3. В блоке **Настройки подписи** нажмите кнопку **Редактировать** .
4. Откроется окно **Сертификат подписи** со списком личных сертификатов.



5. Выберите сертификат.

После выбора сертификат будет автоматически привязан в настройках аккаунта.

При необходимости привязанный сертификат можно заменить или отвязать.

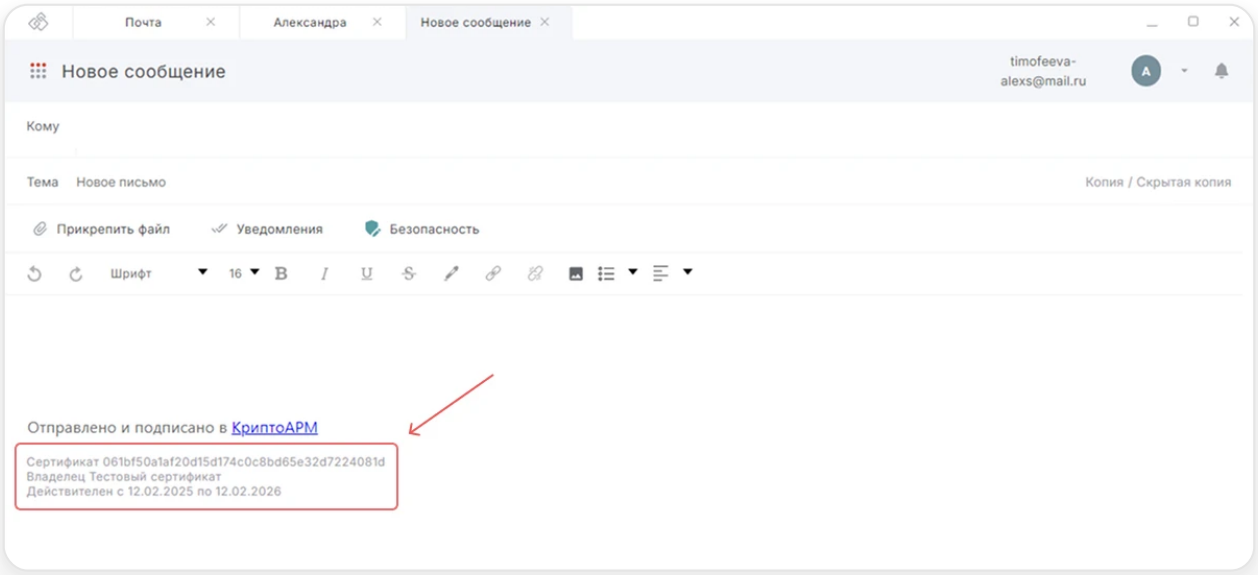
Отображение информации о сертификате

В конце каждого исходящего подписанного письма можно настроить отображение информации о сертификате подписи: отпечаток, имя владельца и срок действия. Это позволит получателям, на устройствах которых не установлено приложение КриптоАРМ, увидеть информацию о сертификате подписи письма.

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Безопасность**.

3. Активируйте переключатель **Отображать информацию об электронной подписи в исходящих письмах**.

Теперь, когда вы отправляете подписанное письмо, данные о сертификате автоматически добавляются в его конец.



Настройки шифрования

Чтобы настроить шифрование исходящих писем:

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Безопасность**.
3. В разделе **Настройки шифрования** выберите один из алгоритмов шифрования: ГОСТ 28147-89, ГОСТ Р 34.12-2015 Магма, ГОСТ Р 34.12-2015 Кузнечик, AES-256-CBC, DES3-CBC.
4. В разделе **Шифрование исходящих сообщений** укажите режим работы:
   - **Использовать сертификат получателя и сертификат подписи почтового аккаунта** — исходящие письма будут шифроваться в адрес сертификатов получателей и в адрес сертификата подписи почтового аккаунта. В папке исходящих писем можно ознакомиться с содержимым отправленного зашифрованного письма.
   - **Использовать только сертификат получателя** — исходящие письма будут шифроваться **только** в адрес сертификатов получателей. В папке исходящих писем невозможно будет расшифровать такое письмо и узнать его содержание.

> 🔐 Алгоритмы ГОСТ доступны при установленном криптопровайдере КриптоПро CSP.

Хранение зашифрованных сообщений

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Безопасность**.
3. В разделе **Хранение входящих зашифрованных сообщений** укажите режим работы:
   - **Хранить входящие сообщения в расшифрованном виде** — все зашифрованные сообщения, которые были хотя бы один раз расшифрованы, будут храниться в расшифрованном виде.
   - **Хранить входящие сообщения в зашифрованном виде** — все зашифрованные сообщения (расшифрованные и зашифрованные), будут храниться в зашифрованном виде.

Скачивание писем

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Безопасность**.
3. В разделе **Скачивание писем** укажите режим работы:
   - **Получать только текст сообщений** — при получении письма будет загружен только его текст. Загрузка вложений начнется только при открытии письма. Выбор этой настройки позволит ускорить процесс получения писем.
   - **Скачивать сообщения полностью** — при получении письмо будет загружено в полном объеме, включая все вложения.

Хранение почты

В приложении доступно два варианта хранения писем:

1. **Локальное хранение на устройстве**
   - Письма удаляются с сервера после загрузки,
   - Письма фильтруются в папку **Сохранённые письма** со всех аккаунтов,
   - Письма отмечаются специальным индикатором ,
2. **Хранение на сервере**
   - Письма остаются в исходной серверной папке
   - Доступны со всех устройств
   - Синхронизируются автоматически

> 💡Чтобы активировать настройку «Хранение почты», необходимо предварительно включить опцию **Скачивать сообщения полностью**.

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Безопасность**.
3. В разделе **Хранение почты** выберите один из вариантов:
    - **Удалять оригиналы писем с почтового сервера** — оригиналы писем будут удаляться с почтового сервера после синхронизации. Все письма данного почтового аккаунта будут храниться на этом устройстве и видны в папке «Сохранённые письма».
    - **Не удалять оригиналы писем с почтового сервера** — данная настройка стоит по умолчанию. Письма не удаляются с почтового сервера автоматически.

Инструкции по теме

- Добавление почтового аккаунта
- Настройка сортировки писем
- Создание подписи (текстовая подпись в конце письма)
- Общие настройки аккаунта

Открыть статью на сайте

Настройки подключения

- Редактирование настроек подключения
- Настройка специальных папок

Редактирование настроек подключения

1. Изменение настройки подключения

> 💡 При смене настроек подключения убедитесь, что выбран правильный способ аутентификации и указаны актуальные адреса серверов.

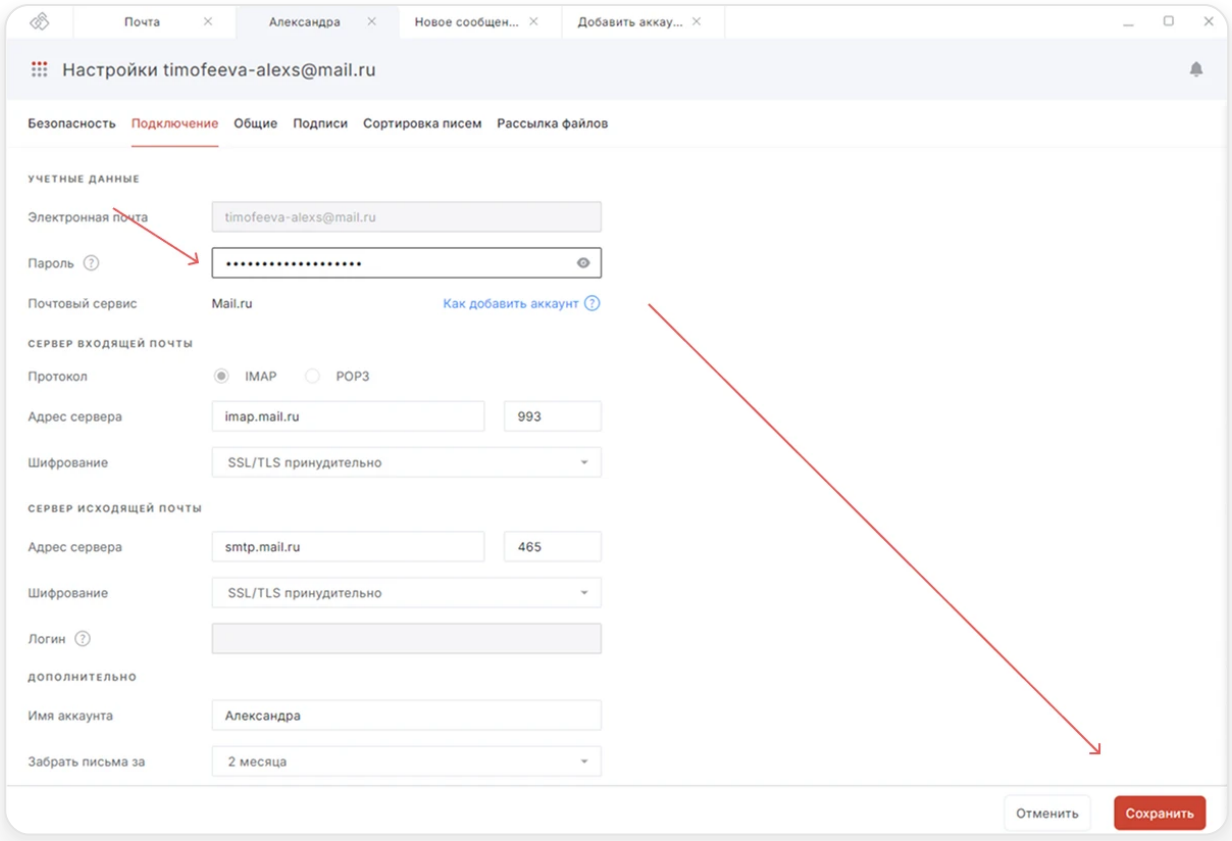
Чтобы изменить настройки подключения:

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Подключение**.
3. Внесите необходимые изменения (например, адреса серверов, протоколы, способ аутентификации).
4. Нажмите кнопку **Сохранить** на появившейся панели действий.

После успешного сохранения подключения начнётся обмен письмами с сервером. Этот процесс может занять некоторое время.

2. Изменение пароля в почтовом аккаунте

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Подключение**.
3. Укажите новый пароль в блоке **Учетные данные**.
4. Нажмите кнопку **Сохранить** на появившейся панели действий



Если подключение с новым паролем пройдёт успешно, начнётся обмен письмами с почтовым сервером. Это может занять некоторое время.

> ⚠️ **Внимание:** Приложение хранит пароль для подключения к почтовому серверу. Если вы измените его здесь, пароль к вашей учётной записи на сервере (Яндекс, Mail.ru, Gmail и другие) **не изменится**. Для смены пароля учётной записи обратитесь к вашему почтовому провайдеру.

Настройка специальных папок

1. Назначение специальных папок

> 📌 **Специальные папки** — это виртуальные папки, которые приложение использует для автоматической сортировки писем (например, «Отправленные», «Спам»). Вы можете **сопоставить** их с существующими папками на вашем почтовом сервере или **создать** локально.

Типы специальных папок:

- Отправленные — для хранения исходящих писем,
- Архив — для долгосрочного хранения важных сообщений,
- Черновики — временное хранилище незавершенных писем,
- Важные — для приоритетной корреспонденции,
- Спам — для удаления нежелательных сообщений,
- Корзина — для восстановления удаленных писем,
- Уведомления — для отслеживания писем с уведомлениями о доставке и прочтении.

Если в аккаунте отсутствуют перечисленные специальные папки, можно создать их вручную с выбором типа синхронизации:

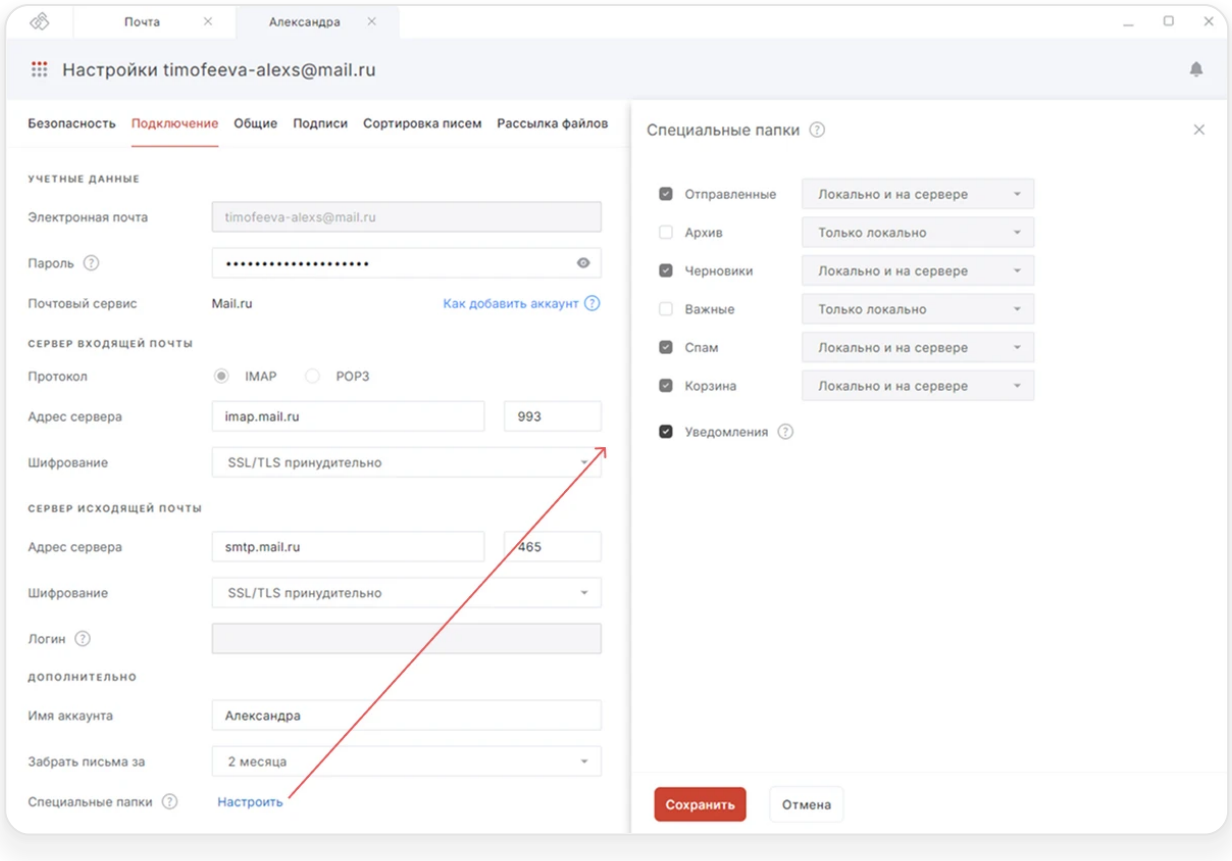
Тип создания	Описание	Протоколы
Локально	Хранится только на устройстве	Доступно для всех протоколов
Локально и на сервере	Синхронизируется с почтовым сервером	Только для IMAP

> 💡 Письма, которые вы поместите в локальную папку, будут удалены с сервера и сохранены на вашем устройстве.

2. Включение специальной папки

Чтобы включить специальную папку:

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Подключение**.
3. В блоке **Специальные папки** нажмите на кнопку **Настроить**.
4. В открывшемся окне отметьте флажками нужные вам специальные папки и выберите тип создания для каждой из них.



5. Нажмите кнопку **Сохранить**.

Выбранные папки появятся в списке папок вашего аккаунта. Письма будут автоматически распределяться в них согласно их типу (например, отправленные письма — в папку «Отправленные»).

> 💡 Чтобы отключить специальные папки, снимите их флажки и сохраните изменения.

Инструкции по теме

- Добавление почтового аккаунта
- Настройки аккаунта для отправки подписанных и зашифрованных писем
- Настройка сортировки писем
- Создание подписи (текстовая подпись в конце письма)
- Общие настройки аккаунта

Открыть статью на сайте

Общие настройки

- Группировка в цепочки
- Автоматическое прочтение при просмотре
- Запрос уведомлений о прочтении и доставке для исходящих писем
- Фильтрация уведомлений о доставке и прочтении исходящих писем
- Отправка уведомлений о прочтении входящих писем
- Инструкции по теме

Группировка в цепочки

> 📌 **Группировка писем** — это отличный способ сделать переписку более организованной. Все письма, касающиеся одной темы и связанные с одними и теми же участниками, будут собраны на одной странице. В папках эти письма также будут отображаться в виде единой строки. Рядом с темой каждого письма будет указана цифра, которая показывает общее количество писем в данной группе.

Чтобы включить или выключить группировку писем в цепочки:

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Общие**.
3. Включите или выключите переключатель **Группировать письма в цепочки**.

Настройки применяются автоматически без дополнительного подтверждения.

Автоматическое прочтение при просмотре

> 📌 По умолчанию в области быстрого просмотра (справа от списка писем) письмо помечается как прочитанное.

Чтобы включить или выключить автоматическое прочтение письма при быстром просмотре:

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Общие**.
3. Включите или отключите переключатель **Отмечать как прочитанное при просмотре в области чтения**.

Настройки применяются автоматически без дополнительного подтверждения.

Запрос уведомлений о прочтении и доставке для исходящих писем

Уведомление о доставке подтверждает доставку сообщения электронной почты в почтовый ящик получателя, но не гарантирует, что оно было просмотрено или прочитано.

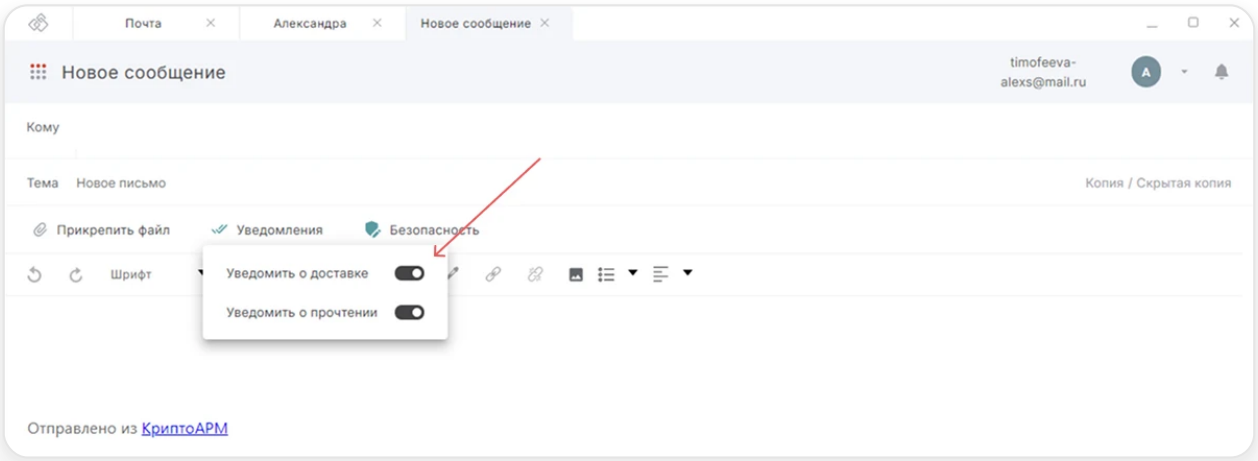
Чтобы узнать, прочитано ли получателем отправленное письмо, можно запросить подтверждение прочтения. Подтверждение будет направлено в виде отдельного письма, в котором будет указана дата и время, когда ваше сообщение было открыто.

Чтобы настроить запрос уведомлений для исходящих писем:

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Общие**.
3. Включите или выключите переключатели:
    - **Запрашивать уведомление о доставке для всех исходящих сообщений**.
    - **Запрашивать уведомление о прочтении для всех исходящих сообщений**.

Настройки применяются автоматически без дополнительного подтверждения.

При открытии формы с новым письмом переключатели будут выставлены в соответствии с указанными настройками.



Фильтрация уведомлений о доставке и прочтении исходящих писем

Для удобной организации почты вы можете настроить автоматическое перемещение служебных уведомлений в специальную папку **Уведомления**.

Существует два способа настройки фильтрации:

- **Способ 1**: Через настройки подключения.

  Включите специальную папку **Уведомления** в настройках подключения аккаунта.

- **Способ 2**: Через общие настройки:

  1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
  2. Перейдите на вкладку **Общие**.
  3. Включите переключатель **Скрывать уведомления** в блоке **Запрос уведомлений**.

Настройки применяются автоматически без дополнительного подтверждения.

Что происходит после активации:

- В вашем аккаунте автоматически создаётся специальная папка **Уведомления**,
- Все письма, содержащие уведомления о доставке и прочтении писем будут фильтроваться в эту папку.

Чтобы отключить автоматическую фильтрацию, выполните одно из следующих действий:

- Деактивируйте переключатель **Скрывать уведомления** в настройках,
- Отключите специальную папку **Уведомления** в настройках подключения.

После отключения все уведомления будут снова поступать в папку **Входящие**.

Отправка уведомлений о прочтении входящих писем

Чтобы настроить отправку уведомлений о прочтении для входящих писем:

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Общие**.
3. Выберите один из вариантов:
   - ✅ **Всегда отправлять уведомления о прочтении для любого полученного сообщения** - для автоматического подтверждения о прочтении для всех писем с запросом.
   - ❓ **Каждый раз спрашивать, следует ли отправить уведомление о прочтении** - при чтении письма будет предложено отправить подтверждения о прочтении.
   - ❌ **Никогда не отправлять уведомления о прочтении** - функция подтверждения о прочтении будет отключена в приложении.

Настройки применяются автоматически без дополнительного подтверждения.

Инструкции по теме

- Добавление почтового аккаунта
- Настройки аккаунта для отправки подписанных и зашифрованных писем
- Настройка сортировки писем
- Создание подписи (текстовая подпись в конце письма)

Открыть статью на сайте

Подписи (контактная информация)

- Создание подписи
- Установка подписи по умолчанию
- Удаление подписи

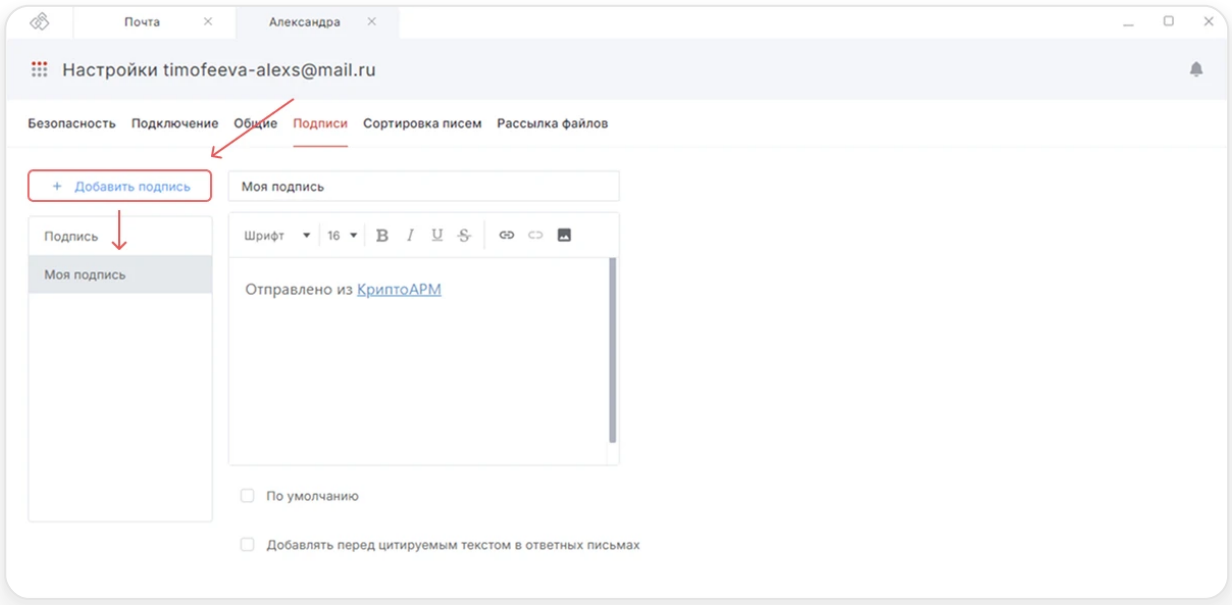
> 📌 **Подпись** - текстовая подпись, которая автоматически добавляется в конец каждого отправляемого письма.

Создание подписи

По умолчанию в приложении задана подпись с текстом **Отправлено из КриптоАРМ** и ссылкой на интернет-магазин cryptoarm.ru.

Чтобы создать подпись:

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Подписи**.
3. Нажмите **Добавить подпись**.



4. Укажите название подписи.

5. Добавьте содержимое подписи:
    - Настройте стиль и размер шрифта.
    - Добавьте изображение. Формат изображения: .jpeg, .jpg, .webp, .gif, максимальный размер — 1024x1024 пикселей, максимальный объем: 2 МБ.
    - Добавьте ссылку. Для добавления ссылки выделите текст, нажмите кнопку **Вставить ссылку** , в появившемся окне укажите адрес ссылки. Вы можете удалить ссылку из подписи, выделив текст и нажав кнопку **Удалить ссылку** .
6. При необходимости установите флаги:
    - **По умолчанию** - подпись будет использоваться по умолчанию во всех исходящих сообщениях.
    - **Добавлять перед цитируемым текстом в ответных письмах** - подпись будет добавляться сразу после текста ответа, а не в конце всех писем в цепочке.

Настройки подписи применяются автоматически без дополнительного подтверждения.

Установка подписи по умолчанию

Чтобы установить подпись по умолчанию:

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Подписи**.
3. Выберите подпись, которую необходимо установить в качестве подписи по умолчанию.
4. Установите флажок **По умолчанию**.

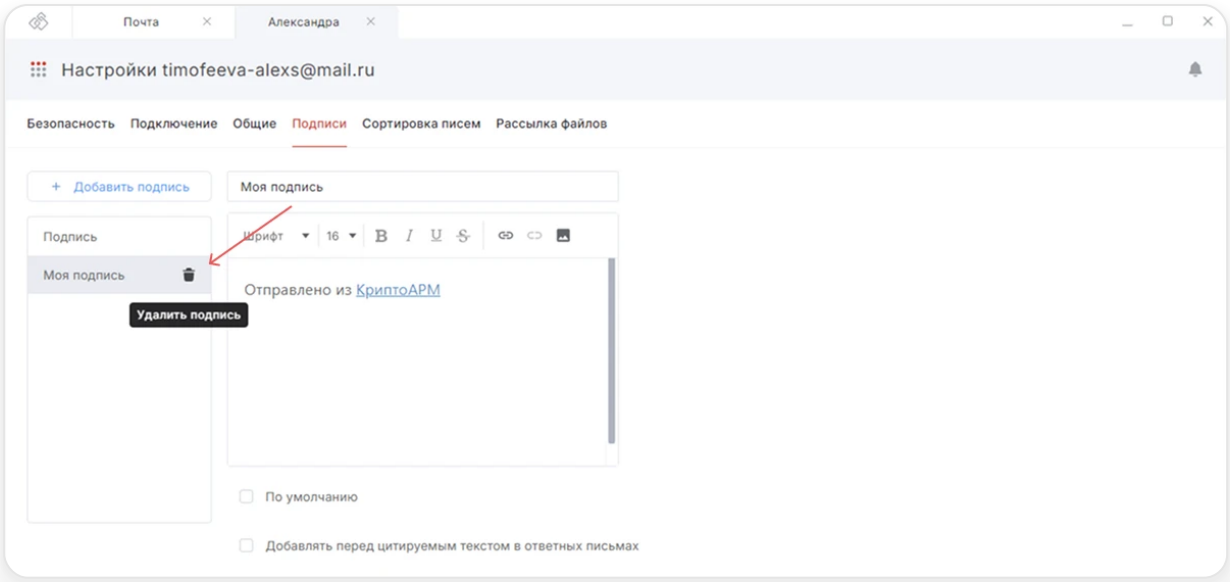
Теперь выбранная подпись будет использоваться по умолчанию во всех исходящих сообщениях

Удаление подписи

> ⚠️ **Действие необратимо.** Подпись удаляется сразу, без возможности восстановления.

Чтобы удалить подпись из приложения:

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Подписи**.
3. Наведите курсор мыши на название подписи и нажмите на всплывающую кнопку **Удалить** .



Подпись будет удалена автоматически без дополнительного подтверждения.

Инструкции по теме

- Добавление почтового аккаунта
- Настройки аккаунта для отправки подписанных и зашифрованных писем
- Настройка сортировки писем
- Общие настройки аккаунта

Открыть статью на сайте

Создание нового письма

- Открытие формы с сообщением
- Добавление получателей
- Настройка отправителя
- Оформление сообщения
- Работа с добавленными вложениями
- Настройка подписи
- Отправка письма
- Возможные ошибки

Открытие формы с сообщением

Чтобы создать новое письмо:

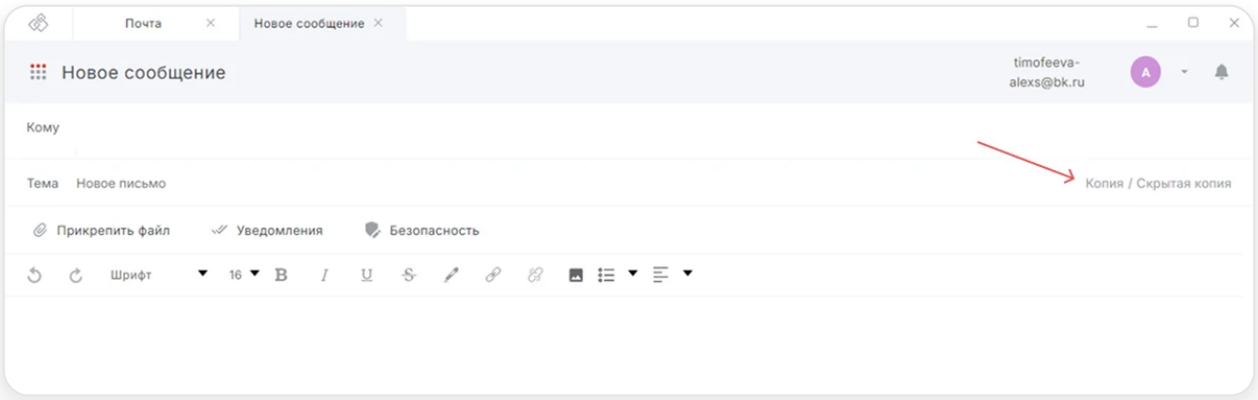
1. Перейдите в раздел **Почта**.
2. Нажмите на кнопку **Новое сообщение** в меню слева.
3. Откроется вкладка с новым письмом.

> 💡 Все неотправленные письма автоматически сохраняются в папке **Черновики**. Чтобы продолжить работу с черновиком, просто откройте его.

Добавление получателей

При открытии окна с новым письмом появляется поле **Кому**. Чтобы активировать поля **Копия** и **Скрытая копия**, просто нажмите на соответствующие кнопки, расположенные на панели **Тема**.

- Поле **Кому** - для добавления основных получателей,
- Поле **Копия** - для добавления получателей, которые должны видеть сообщение,
- Поле **Скрытая копия** - для добавления получателей, чьи адреса не будут видны другим получателям.



1. Ввод получателей вручную

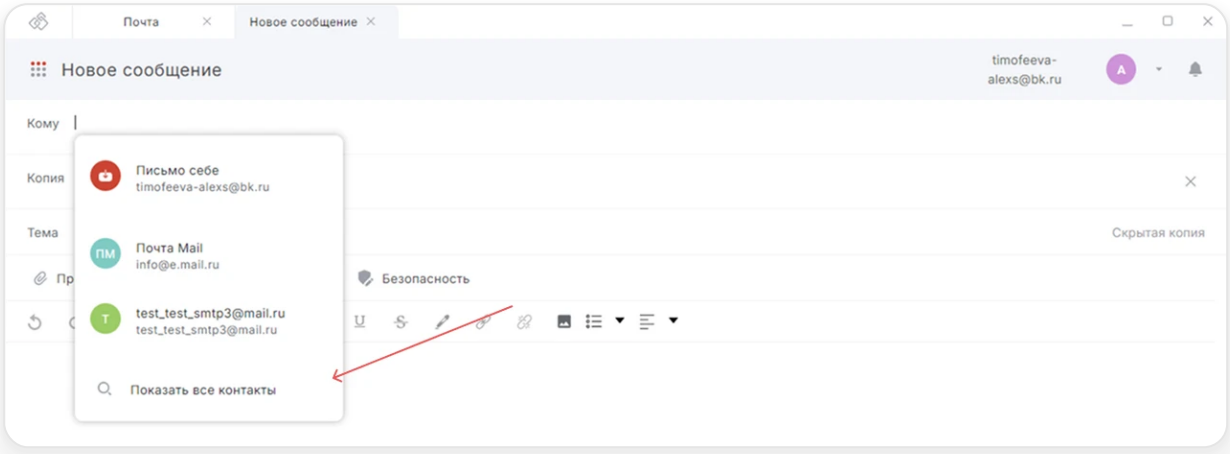
Установите курсор в поле **Кому**, **Копия** или **Скрытая копия** и введите электронные адреса получателей. Адреса можно разделять запятыми, точками с запятой или пробелами.

> 💡 **Совет**: Некорректные адреса подсвечиваются красным. Для быстрого исправления ошибки в адресе можно дважды кликнуть по нему и отредактировать.

2. Выбор из адресной книги

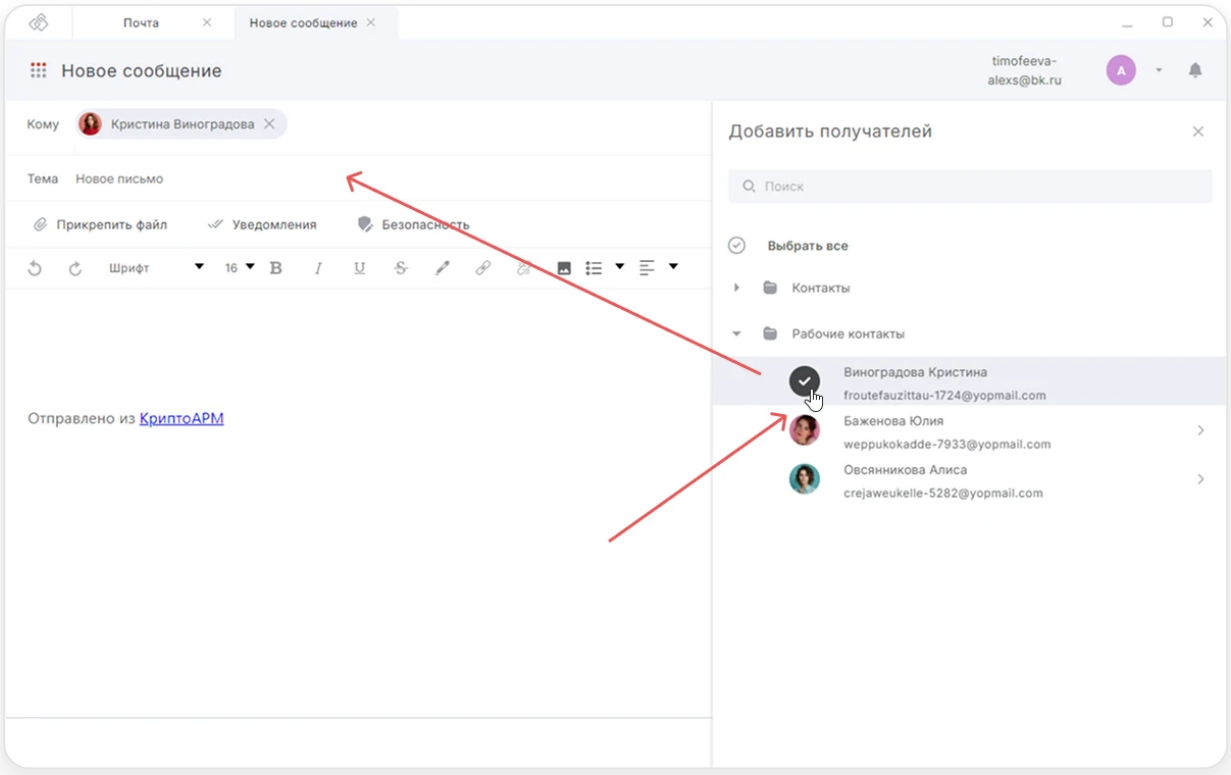
Чтобы выбрать получателей, сохраненных в разделе **Контакты**:

1. Установите курсор в поле **Кому**, **Копия** или **Скрытая копия**.
2. В появившемся меню выберите действие **Показать все контакты**.



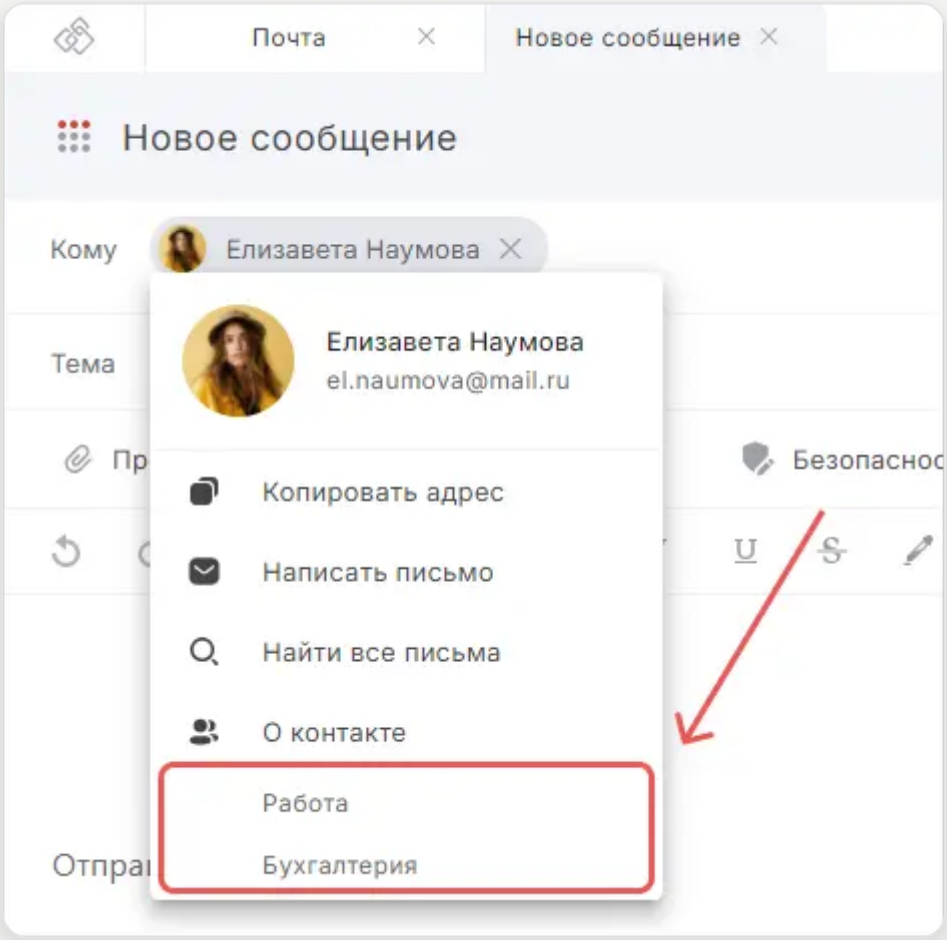
3. Откроется окно со списком адресных книг с контактами. В списке отображаются только контакты с указанными email-адресами. При необходимости можно просмотреть сведения о контакте по кнопке .

4. Выберите один или несколько контактов. Для выбора контакта нажмите на его аватар.



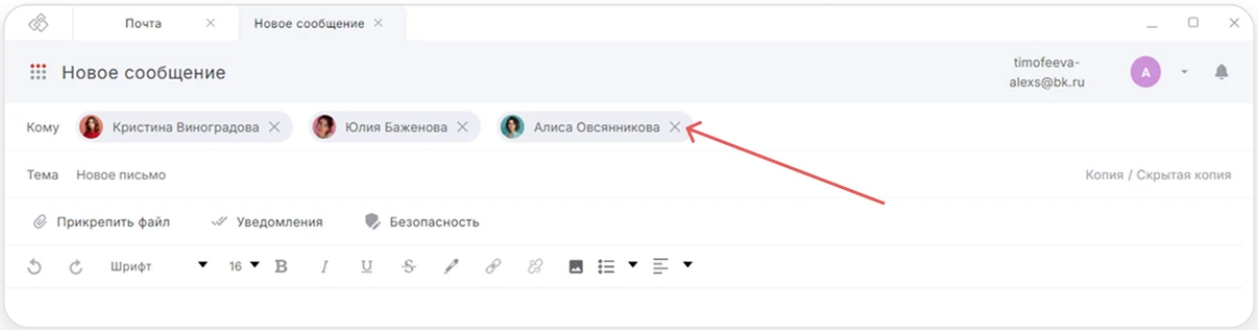
Выбранные контакты автоматически помещаются в соответствующее поле письма.

💡 **Совет**: Если один и тот же контакт присутствует в нескольких адресных книгах, то после выбора получателя отображаются все книги, в которых он найден.



3. Удаление получателя

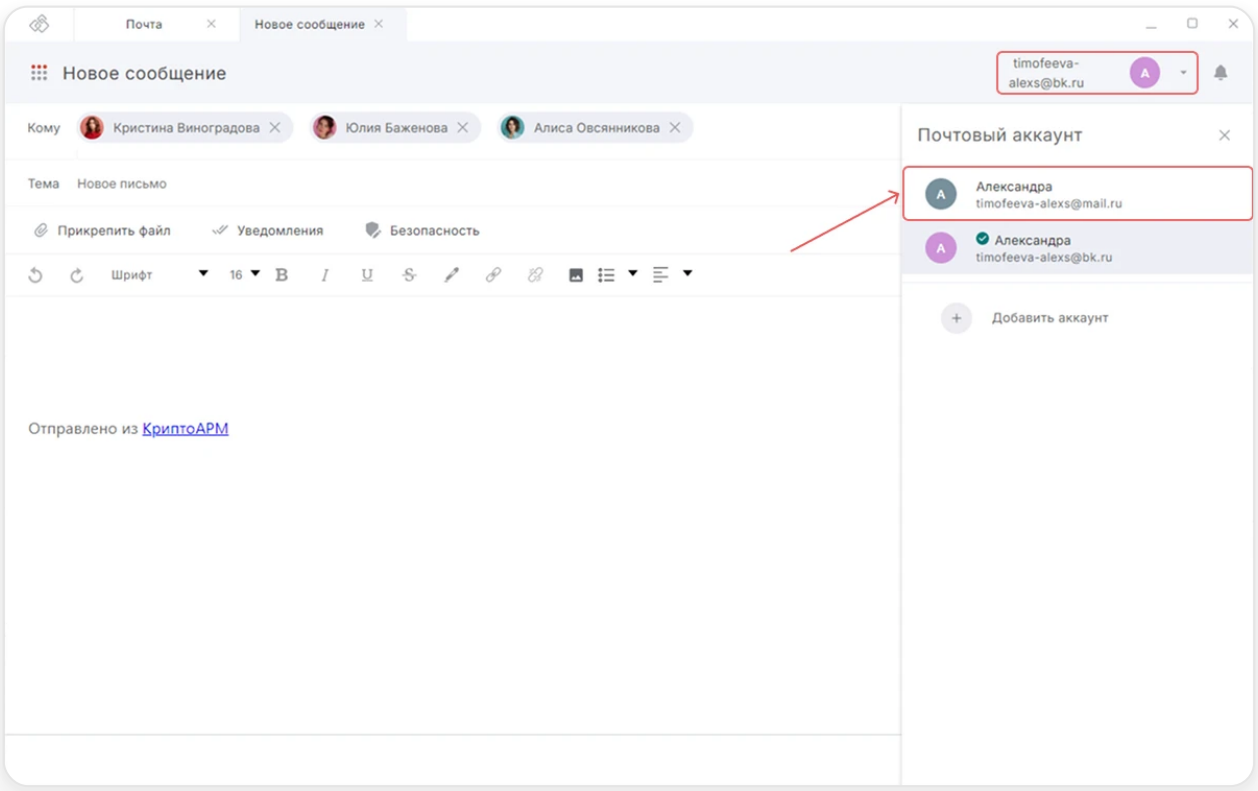
Чтобы удалить получателя из поля **Кому**, **Копия** или **Скрытая копия**, нажмите на кнопку **Удалить** ✕, размещенную рядом с адресом.



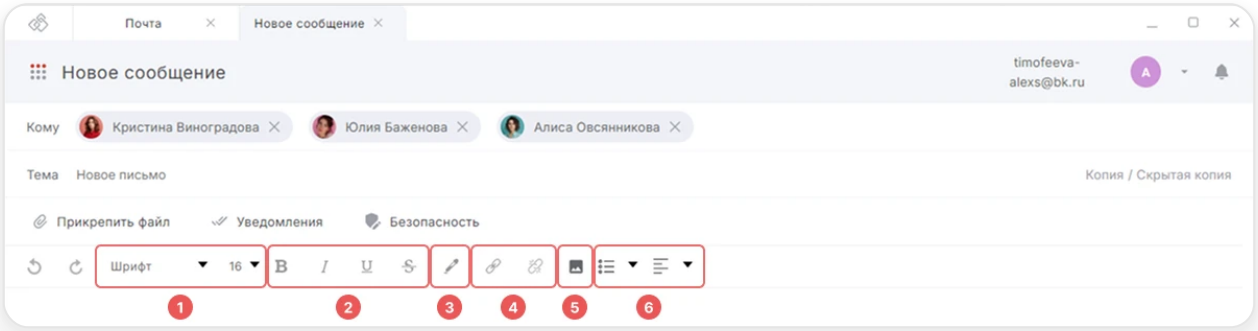
Настройка отправителя

По умолчанию письмо отправляется с активного аккаунта.

Если в приложении добавлено несколько почтовых ящиков, вы можете выбрать тот, который будет использоваться для отправки. Для этого нажмите на имя активного аккаунта в верхнем правом углу и выберите нужный аккаунт в появившемся окне.



Оформление сообщения



1. Выбор стиля и размера шрифта

Чтобы настроить стиль и размер шрифта:

1. Выделите текст письма.
2. На панели действий нажмите на кнопку **Шрифт** и выберите из выпадающего списка необходимый стиль (Arial, Times New Roman, Verdana и другие).
3. Нажмите на кнопку с размером шрифта и выберите из выпадающего списка необходимый размер (от 8pt до 96pt).

2. Выделение текста

Чтобы настроить выделение текста:

1. Выделите текст письма.
2. Выберите необходимый вариант для настройки выделения на панели действий:
   - **Жирный**
   - Курсив
   - Подчёркнутый
   - ~~Зачёркнутый~~

3. Изменение цвета текста и фона

Чтобы настроить цвета текста и фон:

1. Выделите текст письма.
2. Нажмите на кнопку **Выбор цвета** на панели действий.
3. Выберите нужный цвет текст и фона в появившемся окне.

4. Вставка ссылки

Чтобы добавить гиперссылку:

1. Выделите текст письма.
2. Нажмите кнопку **Вставить ссылку** , в появившемся окне укажите адрес ссылки и нажмите **Добавить**. Вы можете удалить ссылку из подписи, выделив текст и нажав кнопку **Удалить ссылку** .

5. Добавление изображения

Чтобы добавить изображение в тело письмо:

1. Установите курсор в то место в тексте письма, куда хотите вставить изображение.
2. Нажмите на кнопку **Вставить изображение** на панели действий.
3. В появившемся окне выберите файл с компьютера с помощью кнопки **Выбрать путь** или вставьте URL. При необходимости настройте ширину и высоту изображение в пикселях.

> 💡 Некоторые почтовые клиенты блокируют загрузку внешних изображений.

6. Списки, отступы и выравнивание

Чтобы добавить список или отступ:

1. Выделите текст письма или начните новый абзац.
2. Нажмите на кнопку **Список** или **Выравнивание текста** .
3. Выберите необходимое действие.

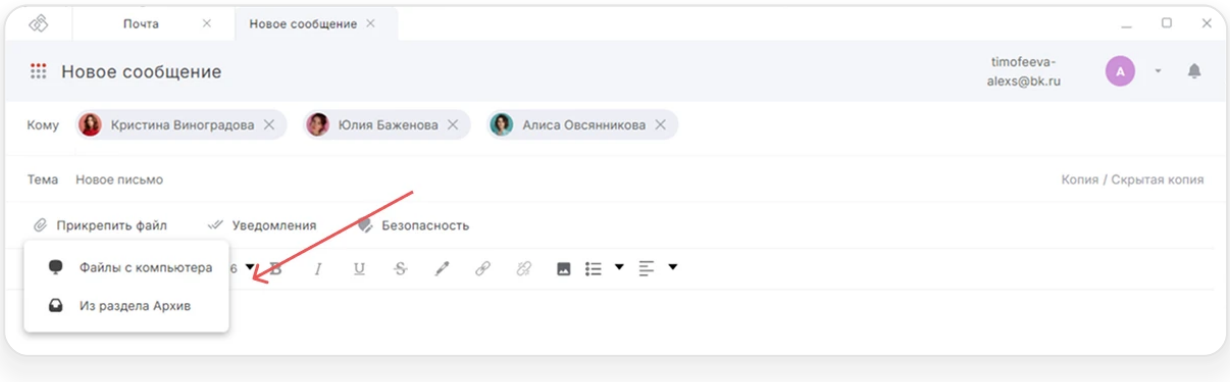
Работа с добавленными вложениями

> 💡 Максимальный размер вложений зависит от почтовых сервисов отправителя и получателя. Даже если ваш сервер поддерживает большие файлы, они могут быть отклонены сервером получателя.

1. Добавление вложений с компьютера

Чтобы добавить вложение:

1. Нажмите на кнопку **Прикрепить файл**.
2. В появившемся меню выберите одно из действие **Файлы с компьютера**.



3. Выберите файлы в появившемся окне файлового менеджера.

После выбора файлы отобразятся в письме.

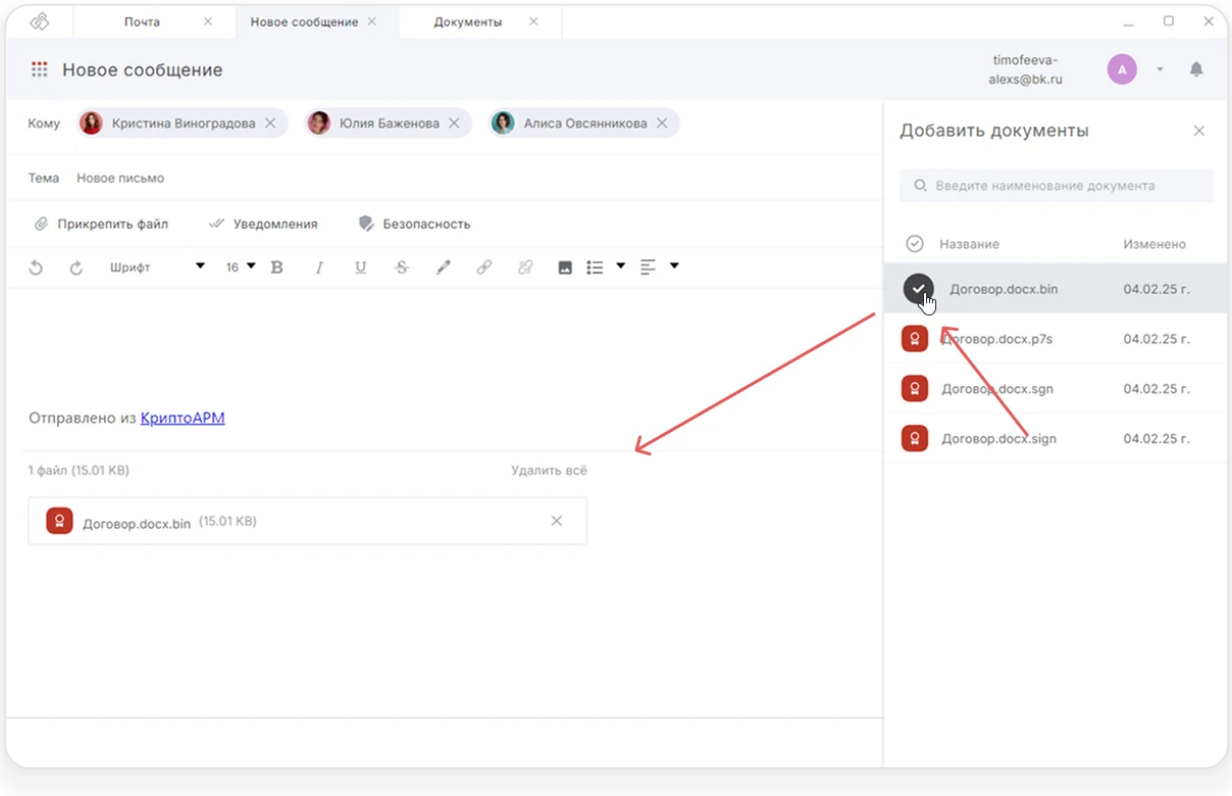
Добавить файлы можно, перетащив их в область создания сообщения. Если перетащить папку с документами, то файлы добавляются списком.

2. Добавление вложений из Архива

> 💡 **Архив** - архивная папка с файлами, созданная в разделе **Документы**.

Чтобы добавить вложение из Архива:

1. Нажмите на кнопку **Прикрепить файл**.
2. В появившемся меню выберите действие **Из раздела Архив**.
3. Откроется окно со списком файлов, сохраненных в папке.



4. Отметьте флажком файлы, которые необходимо добавить к письму. При необходимости воспользуйтесь поиском.

После выбора файлы отобразятся в письме.

3. Удаление вложений

Для удаления ошибочно добавленного вложения нажмите кнопку **Удалить** ✕, размещенную на панели с файлом.

Для удаления всех вложений нажмите **Удалить все**.

4. Просмотр вложения

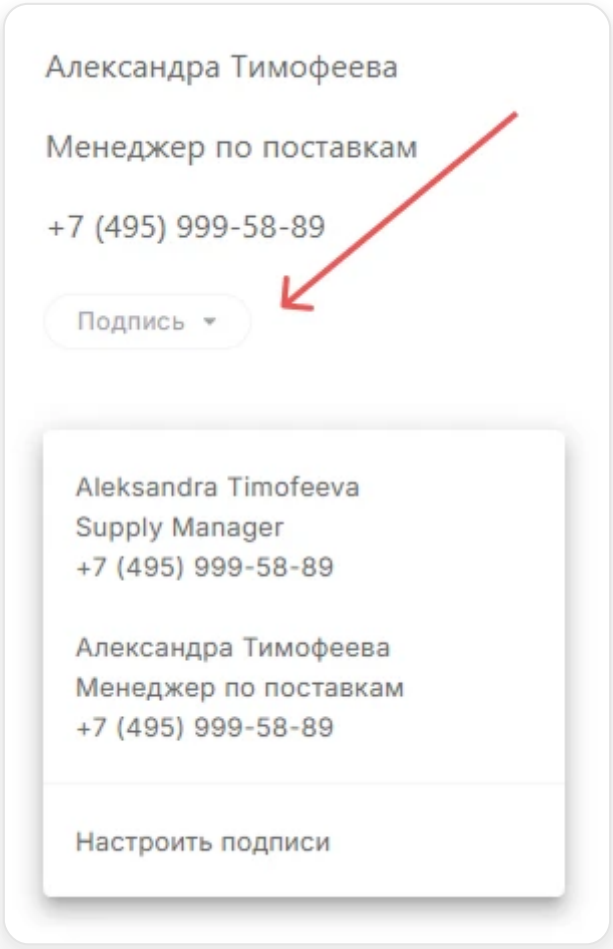
Чтобы просмотреть содержимое добавленного документа, просто нажмите на него. Это действие позволит открыть документ в приложении, которое ассоциируется с его расширением.

Настройка подписи

По умолчанию в приложении задана подпись с текстовкой **Отправлено из КриптоАРМ** и ссылкой на магазин cryptoarm.ru. Подробнее про подписи читайте в инструкции Подпись писем.

Если у вас одна подпись, то она автоматически добавляется при создании сообщения.

Если у вас несколько подписей, то вы можете выбрать нужную подпись с помощью кнопки **Подпись**.



При выборе **Настроить подписи** открывается новая вкладка с настройками почты, где вы можете редактировать подписи.

Отправка письма

Чтобы отправить готовое письмо:

1. Проверьте содержимое письма и получателей.
2. Выставите необходимые настройки:
    - для отправки письма с уведомлением,
    - для отправки защищенного письма.
3. Нажмите кнопку **Отправить**.

Отправленное письмо будет сохранено в папке **Отправленные**.

Возможные ошибки

При возникновении ошибок вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Рекомендуемые действия	Дополнительная информация
Укажите получателей письма в полях Кому, Копия или Скрытая копия	Проверьте заполнение полей	Обязательно должен быть указан хотя бы один получатель в поле "Кому"
Адреса user@aa не распознаны. Проверьте правильность ввода адресов	1. Проверьте правильность написания адресов 2. Убедитесь, что адреса разделены запятыми или точками с запятой 3. Удалите некорректные адреса	Пример корректного формата: username@domain.ru
Не удалось отправить сообщение	1. Проверьте подключение к Интернету 2. Попробуйте отправить письмо позже 3. Перезагрузите приложение	Может возникать при временных проблемах с соединением
Ошибка соединения	1. Проверьте настройки SMTP-сервера исходящей почты 2. Убедитесь в правильности порта и типа шифрования 3. Проверьте логин и пароль для отправки почты	Настройки можно найти в настройках подключения почтового аккаунта

Инструкции по теме

- Отправить подписанное и зашифрованное сообщение
- Отправить письмо с уведомлениями о доставке и прочтении
- Добавить почтовый аккаунт
- Создать контакт
- Посмотреть уведомления

Открыть статью на сайте

Отправка письма с запросом уведомлений о доставке и прочтении

- Об уведомлениях
- Отправка письма с уведомлениями
- Возможные ошибки

Об уведомлениях

В приложении доступна отправка письма со следующими уведомлениями:

1. **Уведомление о доставке**
    - Подтверждает получение письма сервером адресата
    - Не гарантирует, что письмо было просмотрено
    - Приходит сразу после технической доставки
2. **Уведомление о прочтении**
    - Подтверждает факт открытия письма
    - Содержит точную дату и время прочтения
    - Отправляется как отдельное сообщение

> ⚠️ **Важно понимать**:
>
> - Некоторые почтовые системы отправляют уведомления автоматически.
> - Получатель может отключить подтверждения прочтения.
> - Уведомление может прийти при автоматической пометке письма как прочитанного

Отправка письма с уведомлениями

1. Перейдите в раздел **Почта**.
2. Нажмите на кнопку **Новое сообщение** в боковом меню.
3. Откроется вкладка с новым письмом.
4. Добавьте получателей в поле **Кому**, **Копия** или **Скрытая копия** одним из способов:
    - Установите курсор в поле **Кому** и введите электронные адреса получателей,

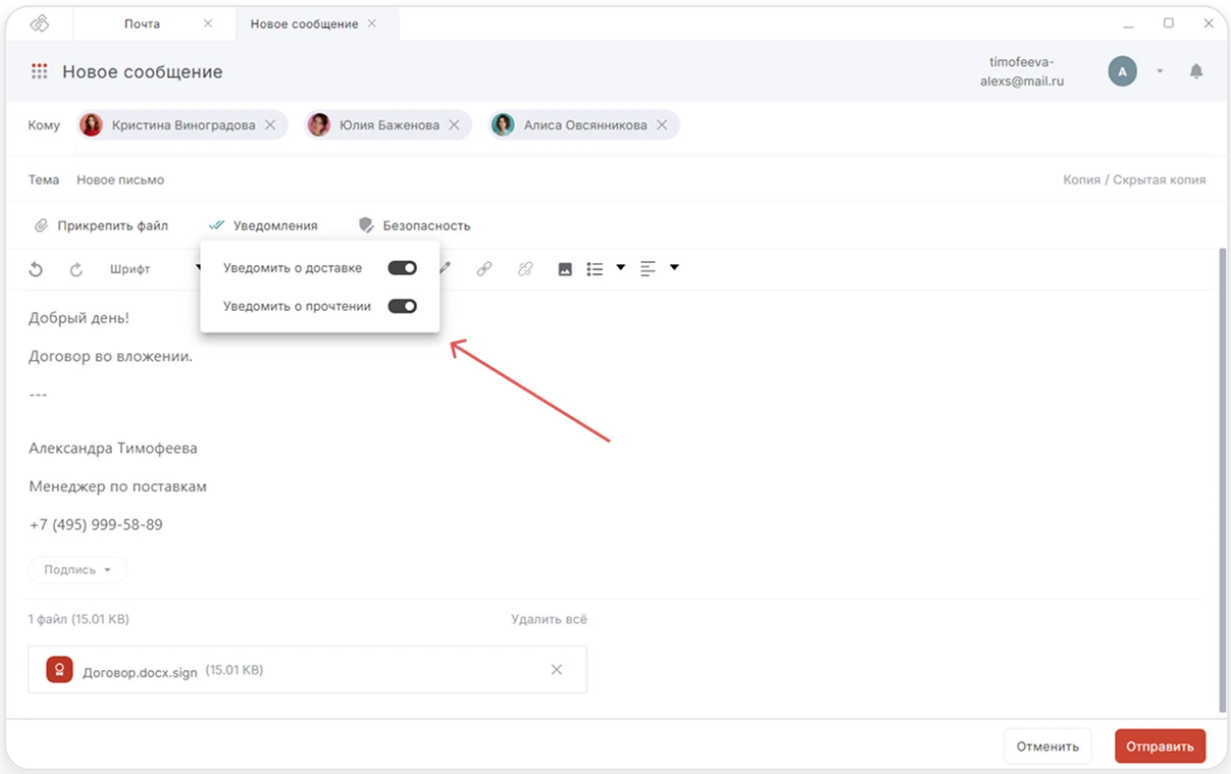
- Выберите получателей из адресной книги. Для этого установите курсор в поле **Кому** и в появившемся меню выберите действие **Показать все контакты**. Откроется окно со списком адресных книг с контактами. В списке отображаются только контакты с указанными email-адресами. Выберите один или несколько контактов. Для выбора контакта нажмите на его аватар.

5. Укажите тему, содержимое и настройте текстовую подпись письма.

6. При необходимости добавьте вложения. Как добавить вложения читайте в инструкции.

7. Выставите настройки для отправки письма с уведомлениями:

   - **Уведомить о доставке**,
   - **Уведомить о прочтении**.



8. При необходимости выставите настройки для отправки защищенного письма.

> **Примечание:** Запрос уведомлений работает и для **подписанных и зашифрованных писем**.

9. Нажмите **Отправить**.

> 💡 **Совет**:
>
> 1. Настройте автоматическую сортировку уведомлений в отдельную папку, чтобы они не смешивались с обычной почтой.
> 2. Настройки для отправки писем с уведомлениями можно заранее установить в Общих настройках почтового аккаунта.

Возможные ошибки

При возникновении ошибок вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Рекомендуемые действия	Дополнительная информация
Ошибка при отправке	1. Проверьте настройки уведомлений о доставке/прочтении 2. Убедитесь, что почтовые серверы получателей поддерживают уведомления о доставке 3. Попробуйте отключить запрос уведомлений	Некоторые почтовые сервисы не поддерживают стандартные уведомления

Инструкции по теме

- Как узнать доставлено ли письмо
- Как узнать прочитано ли письмо
- Отправка подписанного и зашифрованного сообщения
- Добавление почтового аккаунта
- Создание контакта

Открыть статью на сайте

Отправка письма с подписью и шифрованием

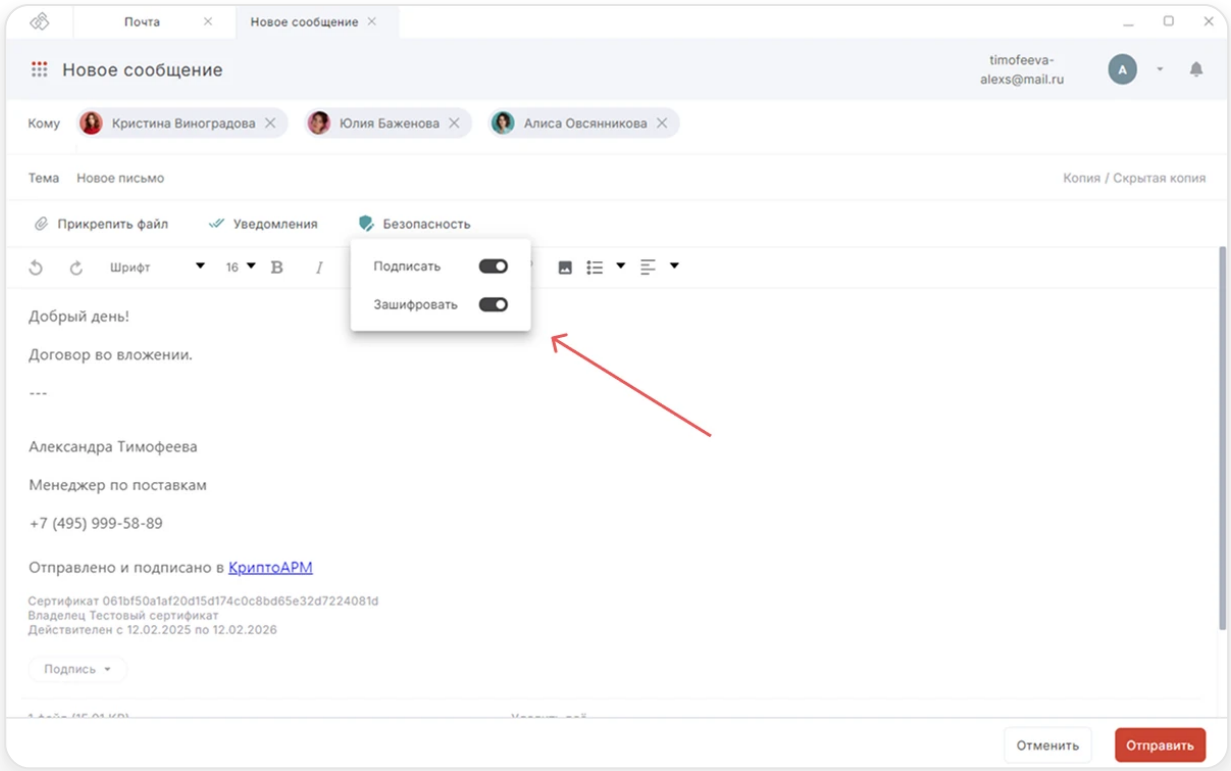
> 💡 **С чего начать**: Чтобы оценить, готово ли ваше рабочее место для работы с почтой, воспользуйтесь Проверкой рабочего места.

Отправка письма с подписью и шифрованием

1. Перейдите в раздел **Почта**.
2. Нажмите на кнопку **Новое сообщение** в боковом меню.
3. Откроется вкладка с новым письмом.
4. Добавьте получателей в поле **Кому**, **Копия** или **Скрытая копия** одним из способов:
   - Установите курсор в поле **Кому** и введите электронные адреса получателей,
   - Выберите получателей из адресной книги. Для этого установите курсор в поле **Кому** и в появившемся меню выберите действие **Показать все контакты**. Откроется окно со списком адресных книг с контактами. В списке отображаются только контакты с указанными email-адресами. Выберите один или несколько контактов. Для выбора контакта нажмите на его аватар.
5. Укажите тему, содержимое и настройте текстовую подпись письма.
6. При необходимости добавьте вложения.

   > 🔍 Как добавить вложения читайте в инструкции.

7. При необходимости выставите настройки для отправки письма с уведомлениями.
8. Выставите настройки для отправки защищенного письма:
   - **Подписать** - для отправки подписанного письма,
   - **Зашифровать** - для отправки зашифрованного письма.

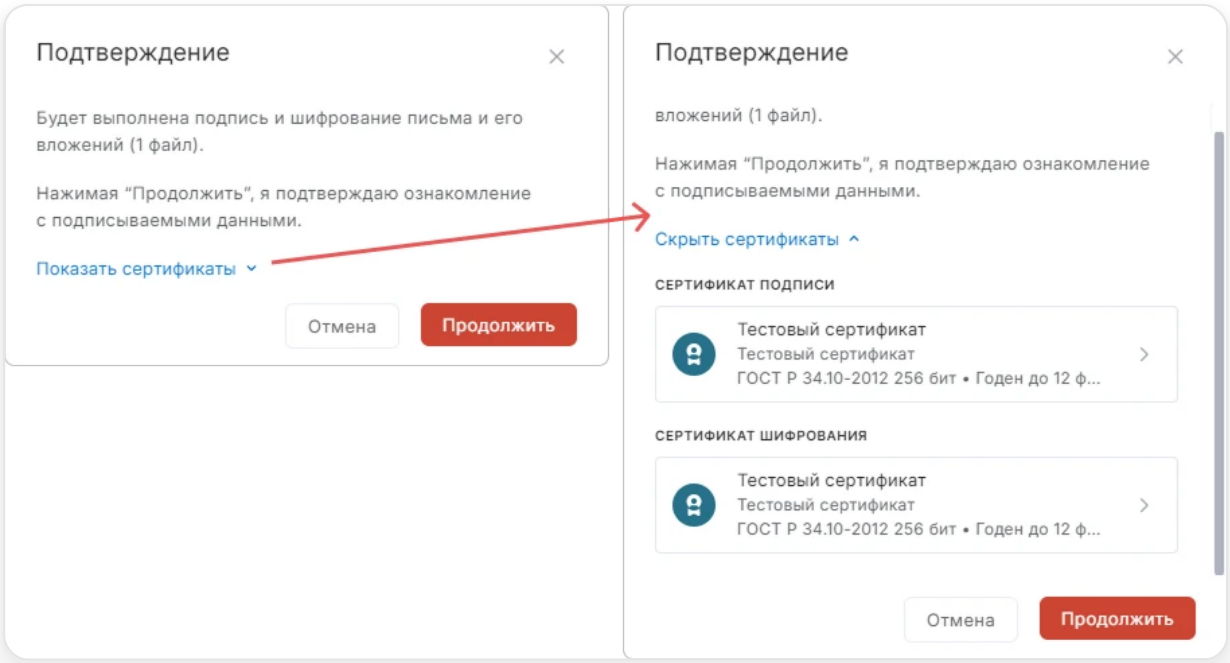


> 💡 **Совет**: Настройки для отправки защищенного письма можно заранее установить в настройках Безопасности почтового аккаунта.

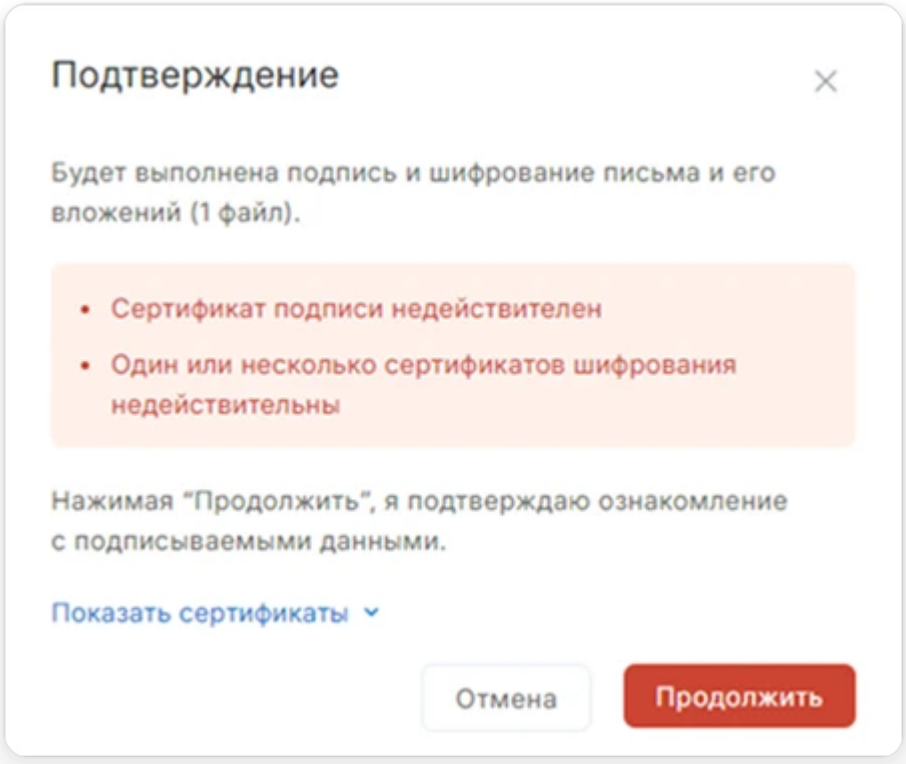
9. Нажмите **Отправить**.
10. Ознакомьтесь со сведениями в окне **Подтверждение**.

    Окно содержит сведения о выполняемых операциях и используемых сертификатах.

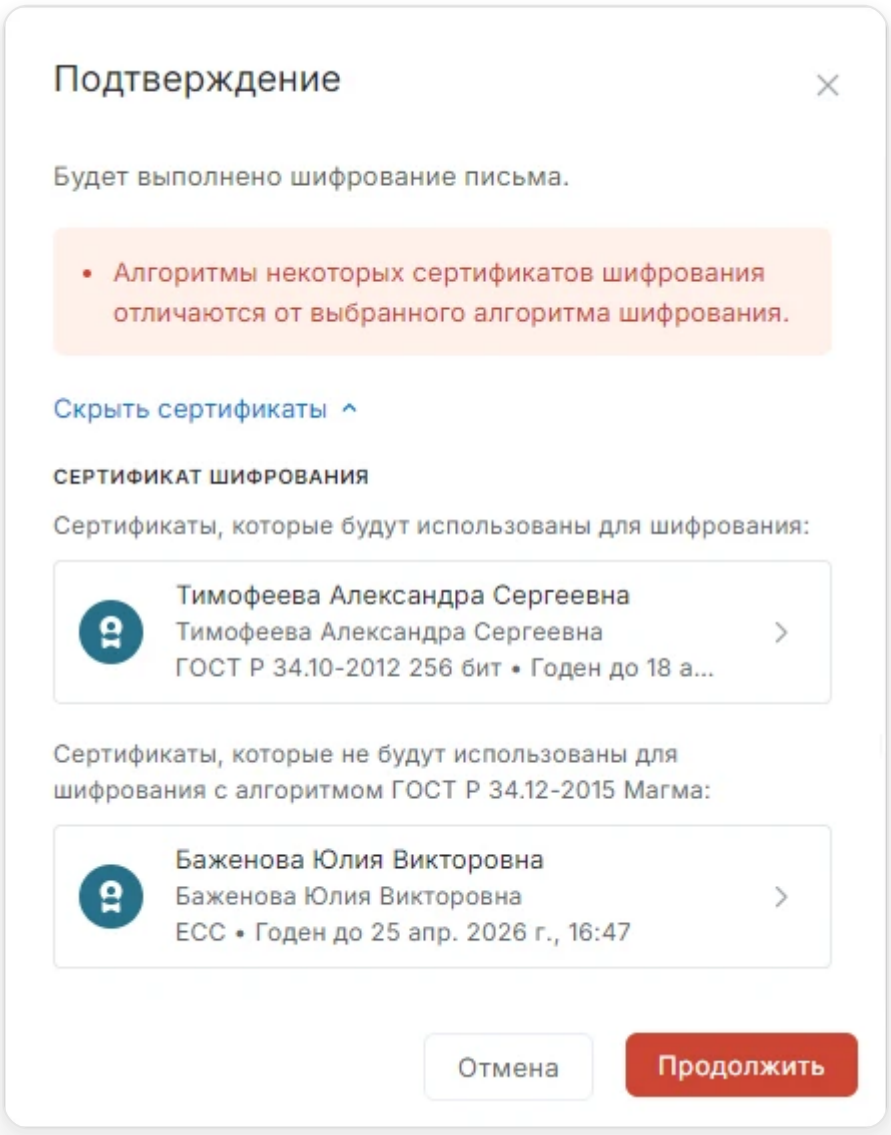
> 💡 **Совет**: Чтобы просмотреть информацию о сертификате подписи, нажмите на кнопку **Показать сертификат**. После этого нажмите на панель с сертификатом.



Если сертификат подписи или сертификаты шифрования окажутся недействительными, в окне появится соответствующее уведомление. В такой ситуации отправка письма не будет заблокирована, однако следует учесть, что получатель может не принять такое письмо.



В случае, если алгоритмы шифрования сертификатов контактов не будут соответствовать настроенному алгоритму шифрования, то письмо будет зашифровано в адрес тех сертификатов, которые соответствуют этому алгоритму. В окне с подтверждением операции отобразится уведомление, а также можно будет ознакомиться со списком сертификатов шифрования:



11. Нажмите кнопку **Продолжить**.

    Нажав «Продолжить» в окне, вы подтверждаете, что ознакомились с подписываемыми данными.

12. При необходимости укажите пароль на контейнер или пин-код на закрытый ключ сертификата.

Дождитесь отправки письма.

Возможные ошибки

При возникновении ошибок вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Причина	Рекомендуемые действия
Для подписи письма выберите сертификат в настройках аккаунта и повторите отправку	Сертификат подписи не выбран в настройках аккаунта	1. Выберите сертификат в настройках Безопасности 2. Повторите отправку
Один или несколько сертификатов отсутствуют. Проверьте наличие сертификатов у получателей.	Отсутствуют сертификаты шифрования у одного или нескольких адресатов	1. Проверьте наличие сертификатов у получателей 2. Добавьте сертификаты к контактам 3. Повторите отправку
Отсутствует необходимый криптопровайдер. Алгоритм открытого ключа сертификата: ГОСТ Р 34.10-2012 256 бит	Отсутствует КриптоПро CSP	Установите КриптоПро CSP и перезапустите приложение КриптоАРМ
Отсутствует СКЗИ КриптоПро CSP. Установите дистрибутив с сайта cryptopro.ru и повторите попытку	Отсутствует КриптоПро CSP	Установите КриптоПро CSP и перезапустите приложение КриптоАРМ
Для операций подписи и расшифрования с использованием ГОСТ алгоритмов требуется лицензия на КриптоАРМ 6	Отсутствует действующая лицензия КриптоАРМ	Установите лицензию КриптоАРМ
Для операций подписи и расшифрования с использованием ГОСТ алгоритмов требуется лицензия на КриптоПро CSP	Отсутствует действующая лицензия КриптоПро CSP	1. Приобретите лицензию КриптоПро CSP 2. Активируйте лицензию в настройках программы

Инструкции по теме

- Проверка рабочего места
- Создание нового письма
- Создание письма с уведомлениями
- Установка КриптоПро CSP на платформу Windows
- Установка КриптоПро CSP на платформу Linux
- Установка личного сертификата
- Привязка сертификата к контакту

Открыть статью на сайте

Действия с письмами

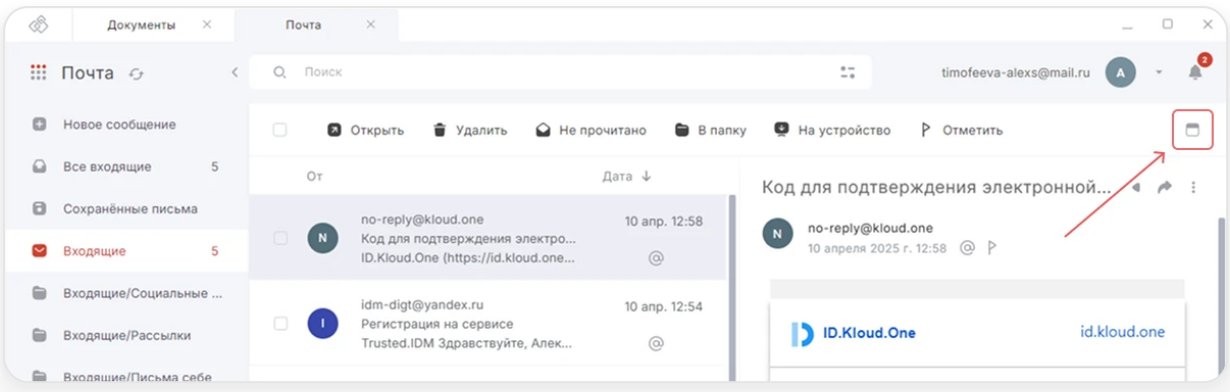
- Чтение письма
- Ответить, Ответить всем, Переслать
- Отметка «Важно»
- Отметить письмо как прочитанное или непрочитанное
- Сохранение письма на устройстве
- Перемещение письма
- Скачивание письма на компьютер
- Печать писем

Чтение письма

1. Чтение в области быстрого просмотра

Чтобы открыть письмо в области быстрого просмотра:

1. Перейдите в раздел **Почта**.
2. Выделите письмо в списке писем.
3. Нажмите кнопку **Просмотр** на панели действий.
4. Справа от списка писем откроется область просмотра письма.

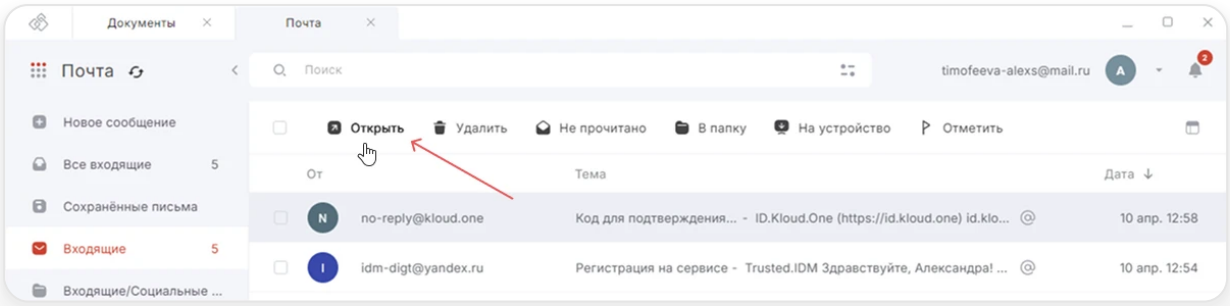


2. Чтение в новой вкладке

Чтобы открыть письмо в новой вкладке:

1. Перейдите в раздел **Почта**.
2. Выполните действие одним из способов:
    - Выделите письмо в списке писем и нажмите кнопку **Открыть** на панели действий.

- Дважды кликните по панели с письмом.

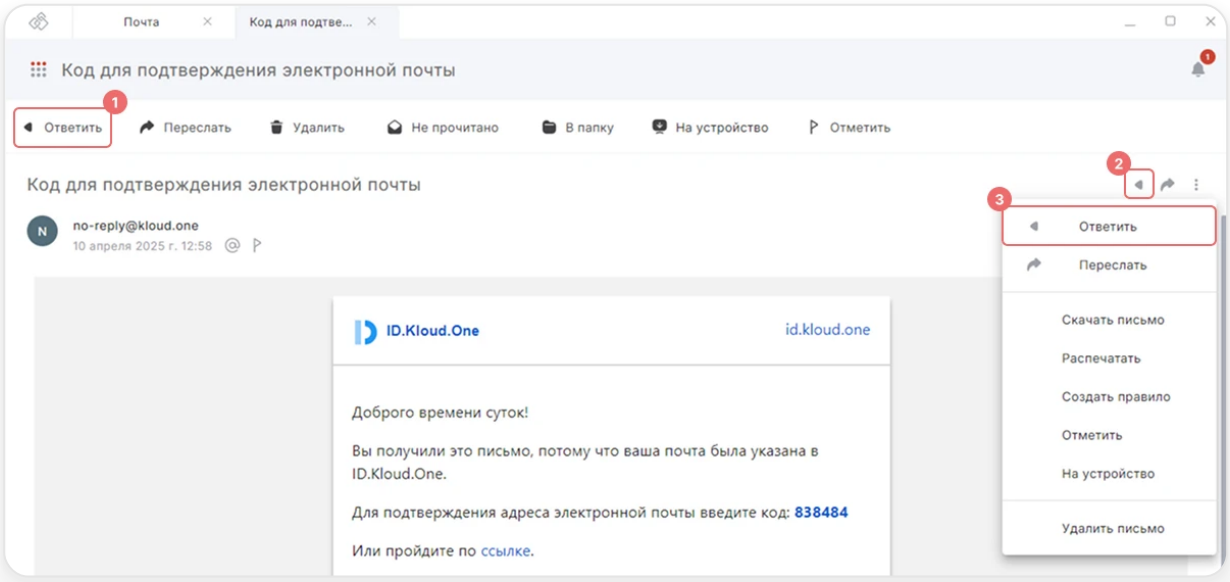


3. Откроется новая вкладка с письмом.

Ответить, Ответить всем, Переслать

1. Ответить и Ответить всем

1. Перейдите в раздел **Почта**.
2. Откройте письмо, на которое нужно ответить.
3. Нажмите на кнопку **Ответить** или **Ответить всем**:
   - На верхней панели действий,
   - На кнопки или , размещенные справа от темы письма,
   - В меню действий, которое вызывается по кнопке **Еще** .



4. Откроется окно с новым сообщением.
5. Заполните необходимые поля и отправьте письмо.

💡 При ответе на зашифрованное письмо автоматически включается настройка **Зашифровать**. Это гарантирует, что все ответы на зашифрованные сообщения также будут защищены, обеспечивая безопасность и конфиденциальность переписки.

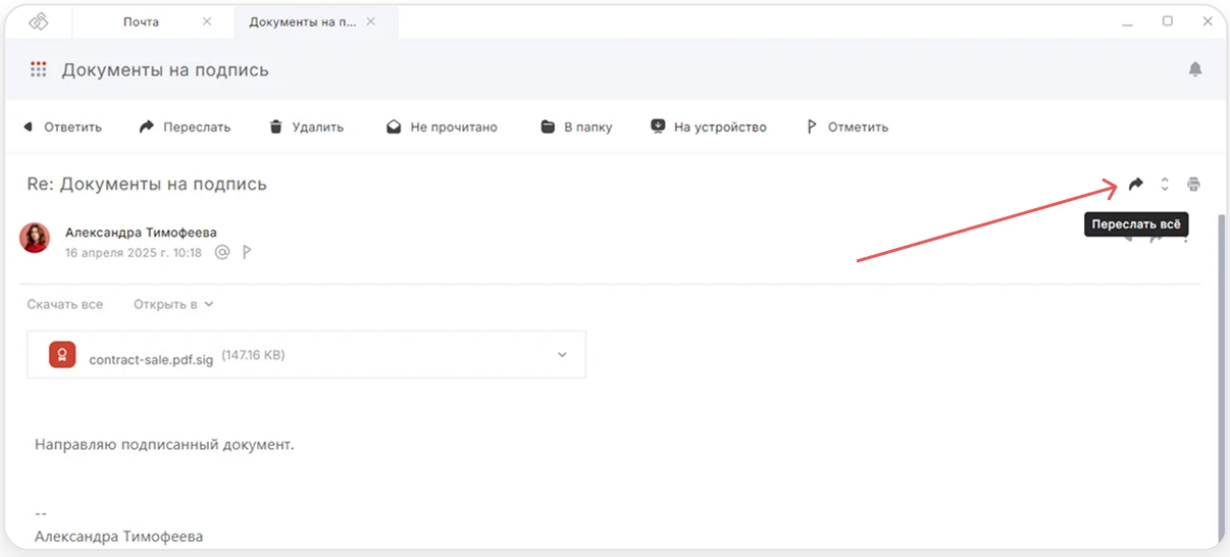
2. Переслать письмо

1. Перейдите в раздел **Почта**.
2. Откройте письмо, которое нужно переслать.
3. Нажмите на кнопку **Переслать**:
   - На верхней панели действий,
   - На кнопку , размещенную справа от темы письма,
   - В меню действий, которое вызывается по кнопке **Еще** .
4. Откроется окно с новым сообщением.
5. Заполните необходимые поля и отправьте письмо.

3. Переслать цепочку писем

💡 **Совет**: Чтобы письма объединялись в цепочки, активируйте функцию просмотра в виде цепочек.

1. Перейдите в раздел **Почта**.
2. Откройте цепочку, которую нужно переслать.
3. Нажмите на кнопку **Переслать все** , размещенную на панели с темой цепочки.



4. Откроется окно с новым сообщением.

5. Заполните необходимые поля и отправьте письмо.

Отметка «Важно»

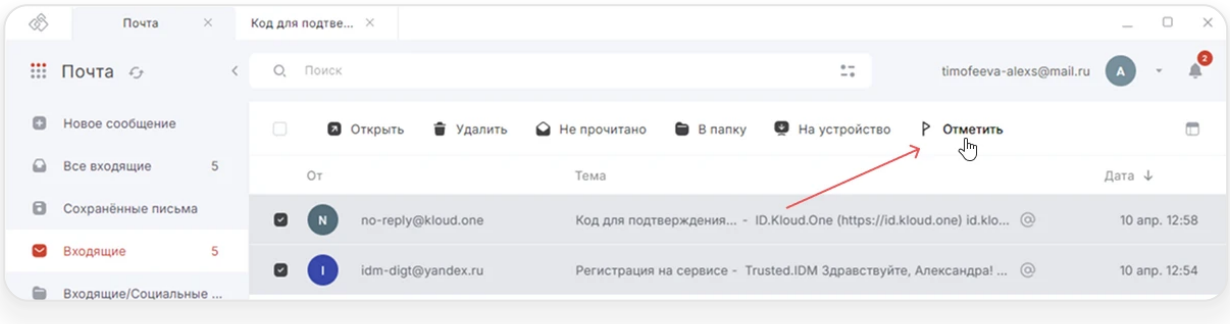
Флаг **Важно** позволяет выделять ключевые сообщения среди общей переписки. Эта функция особенно полезна для отметки срочных писем, выделения важной деловой корреспонденции, организации рабочего процесса с электронной почтой.

> 💡 **Совет**: В расширенном поиске по письмам есть возможность установить фильтр для отметки «Важно».

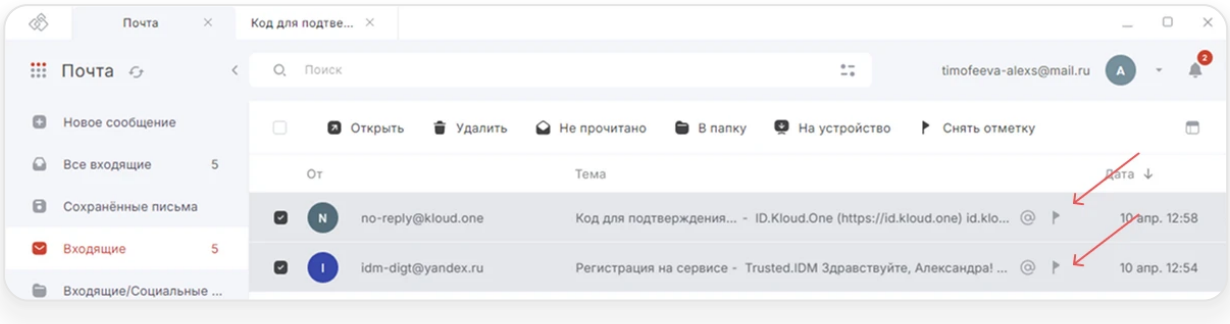
1. Отметка «Важно» в списке писем

Чтобы отметить письмо флагом «Важно» в списке писем:

1. Перейдите в раздел **Почта**.
2. Выделите одно или несколько писем в списке.
3. Нажмите на кнопку **Отметить** на панели действий.



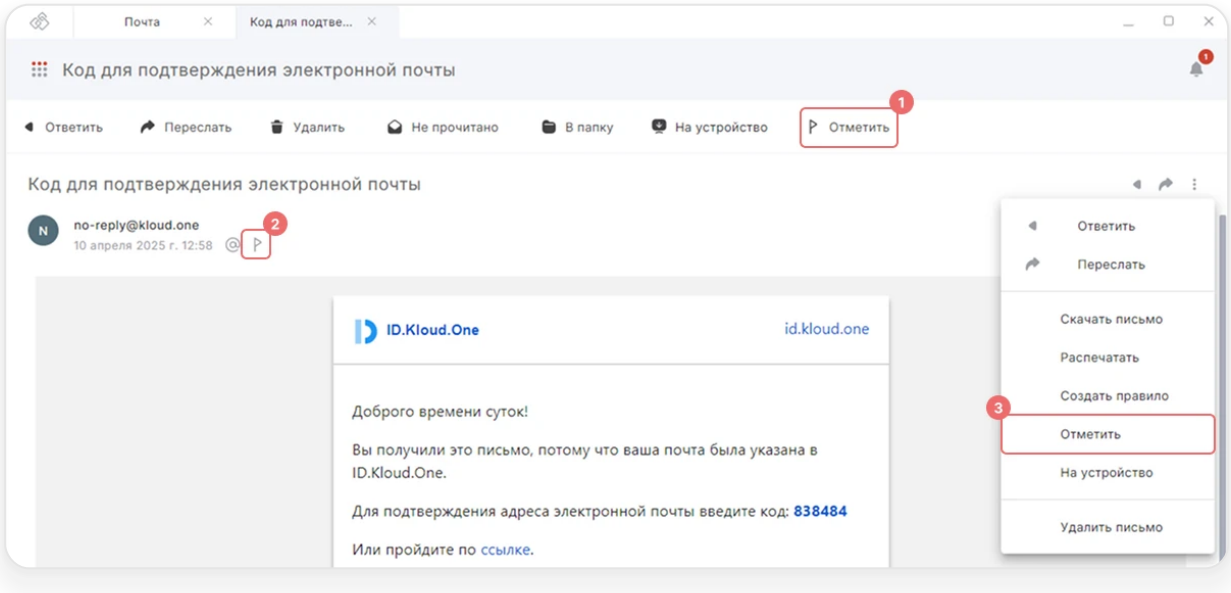
На панели с письмом устанавливается соответствующая отметка. Кнопка **Отметить** меняется на кнопку **Снять отметку**.



2. Отметка «Важно» при чтении письма

Чтобы отметить письмо флагом «Важно» при чтении письма:

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Нажмите на кнопку **Отметить**:
   - На панели действий,
   - На кнопку , размещенную рядом с темой письма,
   - В меню действий, которое вызывается по кнопке **Еще** .



3. Удаление отметки «Важно»

Чтобы снять пометку «Важно» с письма в списке, выделите это письмо и нажмите на кнопку **Снять отметку**, расположенную на панели действий.

Чтобы снять отметку «Важно» при чтении письма, нажмите:

- На кнопку **Снять отметку**, расположенную на панели действий,
- На кнопку , размещенную рядом с темой письма,
- На кнопку **Снять отметку**, в меню действий, которое вызывается по кнопке **Еще** .

Отметить письмо как прочитанное или непрочитанное

1. Отметка в списке писем

Чтобы отметить одно или несколько писем в списке писем:

1. Перейдите в раздел **Почта**.
2. Выделите одно или несколько писем в списке.
3. Нажмите на кнопку **Не прочитано** или **Прочитано** на панели действий.

2. Отметка при чтении письма

Чтобы отметить письмо как прочитанное или непрочитанное при чтении письма:

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Нажмите на кнопку **Не прочитано** или **Прочитано** на панели действий.

Сохранение письма на устройстве

1. Как работает сохранение писем

В приложении доступно два варианта хранения писем:

1. **Локальное хранение на устройстве**
    - Письма удаляются с сервера после загрузки на устройство,
    - Письма фильтруются в папку **Сохранённые письма** со всех аккаунтов,
    - Письма отмечаются специальным индикатором .
2. **Хранение на сервере**
    - Письма остаются в исходной серверной папке,
    - Доступны со всех устройств,
    - Синхронизируются автоматически.

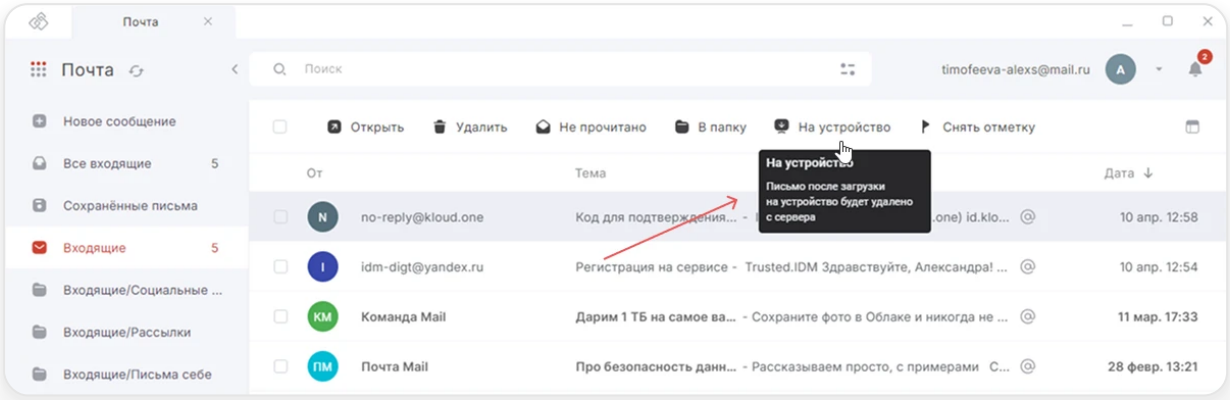
Особенности работы:

- После сохранения письмо доступно в исходной папке и виртуальной папке "Сохранённые письма",
- Оригинал письма на сервере удаляется,
- Для возврата на сервер требуется активное подключение к почтовому аккаунту,
- Размер локально хранимых писем учитывается в общем объеме данных приложения.

2. Сохранение в списке писем

Чтобы переместить одно или несколько писем с почтового сервера на устройство или наоборот:

1. Перейдите в раздел **Почта**.
2. Выделите одно или несколько писем в списке.
3. Нажмите на кнопку:
   - **На устройство** - для переноса с сервера
   - **На сервер** - для возврата на сервер.



3. Сохранение при чтении письма

Чтобы переместить письмо с почтового сервера на устройство или наоборот:

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Выполните действие одним из способов:
   - Нажмите на кнопку **На устройство**/**На сервер**, размещенную на панели действий,
   - Выберите действие **На устройство**/**На сервер**, в меню действий, которое вызывается по кнопке **Еще** ⋮ .

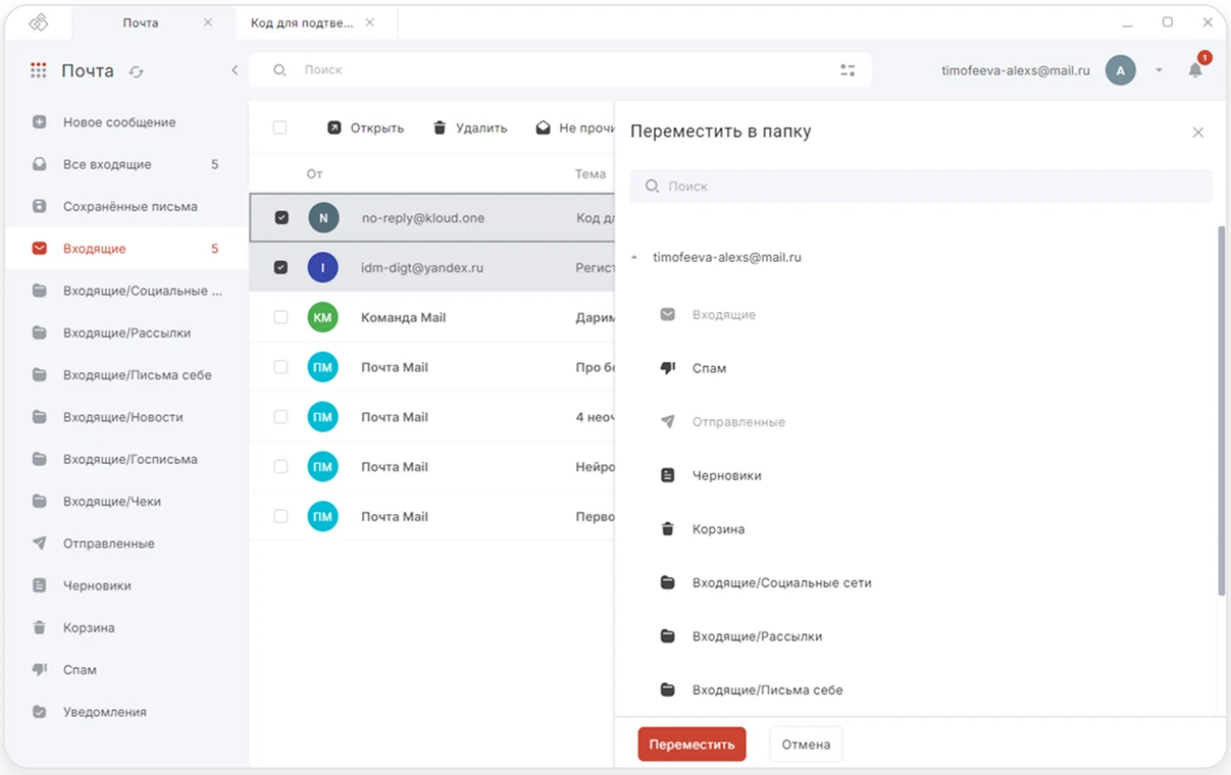
Перемещение письма

1. Перемещение в списке писем

Чтобы переместить одно или несколько писем в списке:

1. Перейдите в раздел **Почта**.
2. Выделите одно или несколько писем в списке.
3. Нажмите на кнопку **В папку** на панели действий.

4. Откроется окно **Переместить в папку**.



5. Выберите папку, в которую необходимо переместить письма.

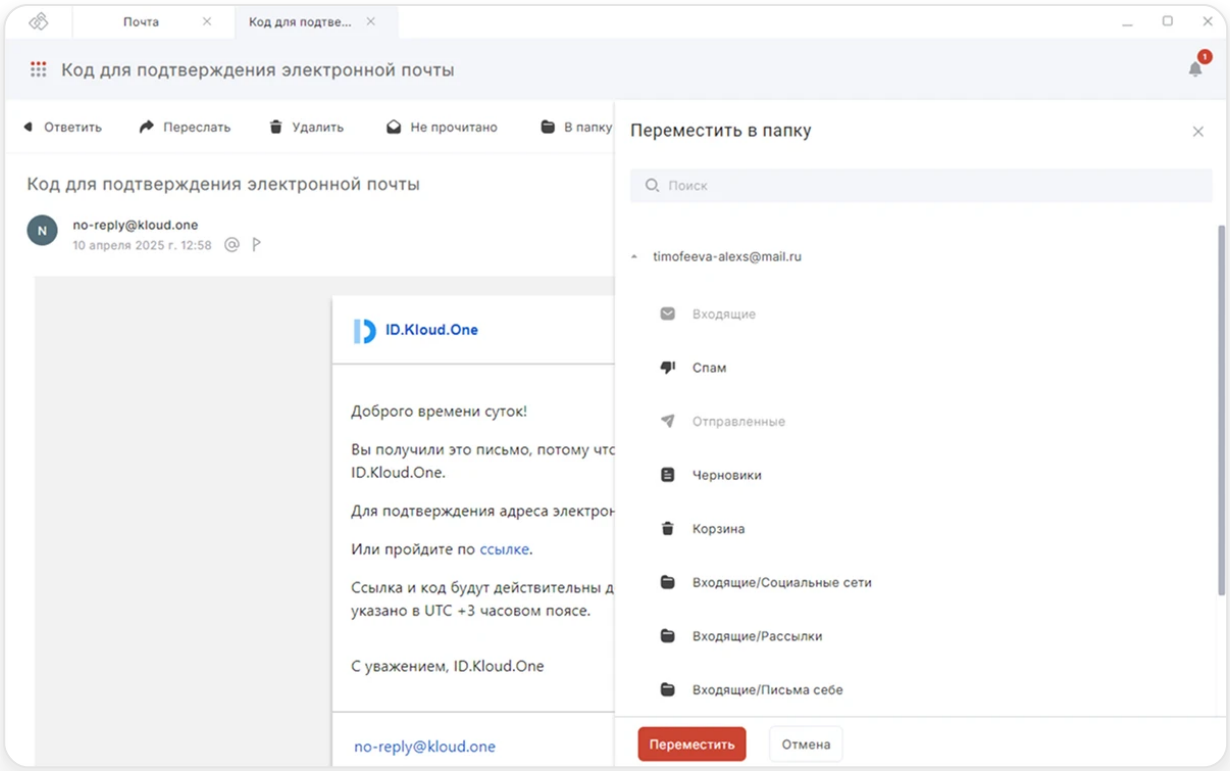
6. Нажмите **Переместить**.

2. Перемещение при чтении письма

Чтобы переместить письмо на вкладке просмотра:

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Нажмите на кнопку **В папку**.

4. Откроется окно **Переместить в папку**.



5. Выберите папку, в которую необходимо переместить письмо.
6. Нажмите **Переместить**.

> 💡При перемещении письма в специальную локальную папку:
>
> 1. Письмо удаляется из исходной серверной папки.
> 2. Создаётся локальная копия письма.

Скачивание письма на компьютер

Чтобы скачать письмо на компьютер:

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Вызовите меню действий с письмом по кнопке **Еще** ⋮.
4. Выберите действие **Скачать письмо**.
5. Укажите место для сохранения файла с письмом.

Письмо скачивается в формате .eml.

Печать писем

1. Распечатать письмо

Чтобы распечатать письмо:

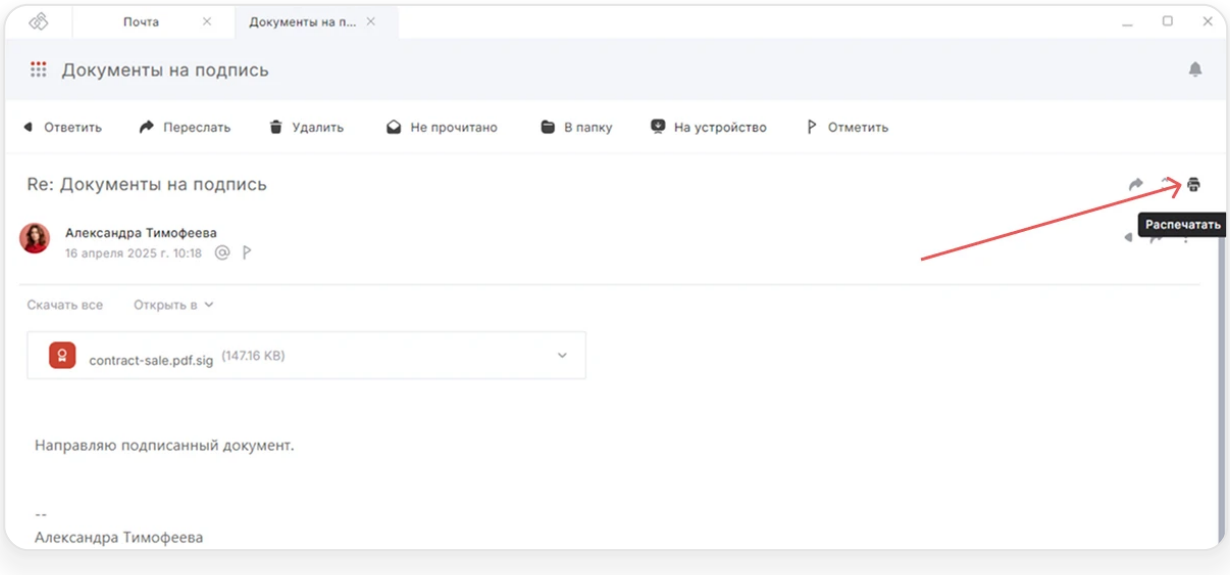
1. Откройте письмо.
2. Вызовите меню действий с письмом по кнопке **Еще** .
3. Выберите действие **Распечатать**.
4. Откроется окно с печатной формой письма.

2. Распечатать цепочку писем

> 💡 **Совет**: Чтобы письма объединялись в цепочки, активируйте функцию просмотра в виде цепочек.

Чтобы распечатать цепочку писем:

1. Откройте цепочку писем.
2. Нажмите на кнопку **Распечатать** , размещенную на панели с темой цепочки.



3. Откроется окно с печатной формой цепочки писем.

Инструкции по теме

- Отправка подписанного и зашифрованного сообщения
- Отправка письма с уведомлениями о доставке и прочтении

- Как узнать доставлено ли письмо
- Как узнать прочитано ли письмо
- Добавление почтового аккаунта
- Создание контакта

Открыть статью на сайте

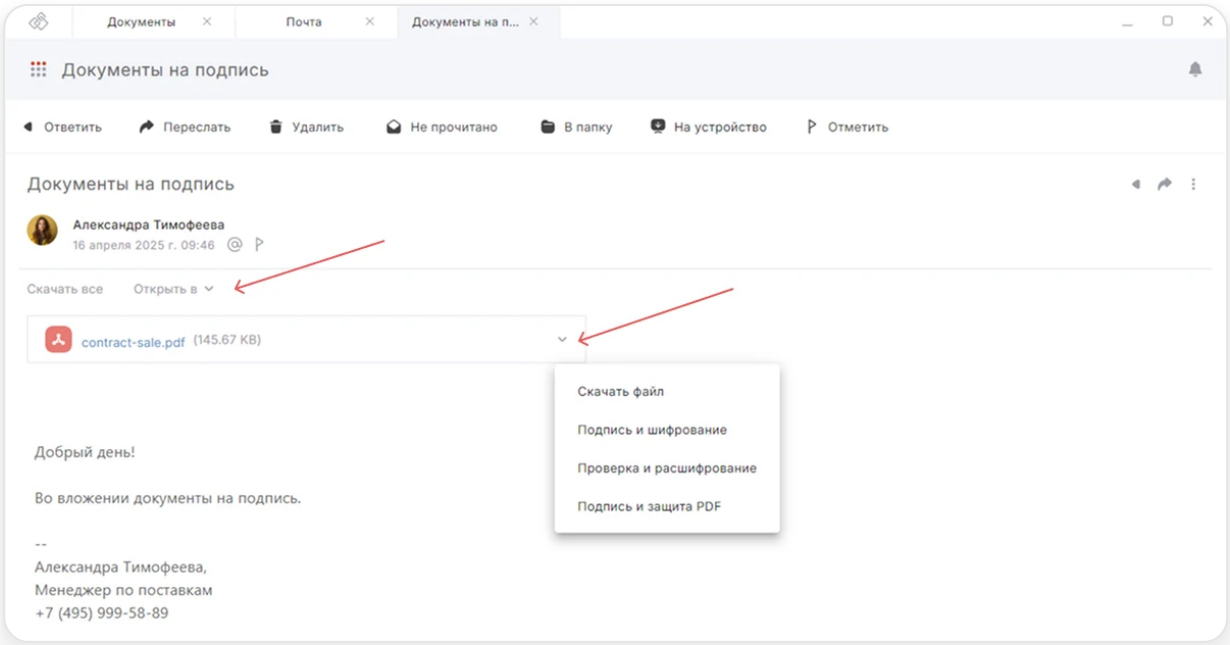
Работа с вложениями в письмах

- Открытие вложения из письма в «Подпись и шифрование», «Проверка и расшифрование» или «Подпись и защита PDF»
- Скачивание вложения на компьютер
- Скачивание всех вложений в одном архиве
- Открытие вложенного файла
- Инструкции по теме

Открытие вложения из письма в «Подпись и шифрование», «Проверка и расшифрование» или «Подпись и защита PDF»

> 💡 Если в письме есть вложенные файлы, то в списке оно будет отмечено специальным индикатором в виде значка **Скрепка**. .

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Дождитесь скачивания вложений, если у вас активна настройка **Получать только текст сообщений**.
4. Выполните действие одним из способов:
    - Вызовите меню действий с вложением по кнопке **Еще** и выберите в меню один мастеров.
    - Вызовите меню действий для всех вложений по кнопке **Открыть в** и выберите в меню один мастеров.



Откроется новая вкладка, на которой вы увидите выбранный мастер с добавленным в него файлом из письма.

> 💡 **Совет**: Для проверки отсоединенной подписи добавьте в мастер исходный документ и файл подписи.

Скачивание вложения на компьютер

> 💡 **Совет**: В расширенном поиске есть возможность установить фильтр для писем с вложениями.

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Вызовите меню действий с вложением по кнопке **Еще** .
4. Выберите действие **Скачать файл**.
5. Укажите путь для сохранения файла в окне файлового менеджера.

Скачивание всех вложений в одном архиве

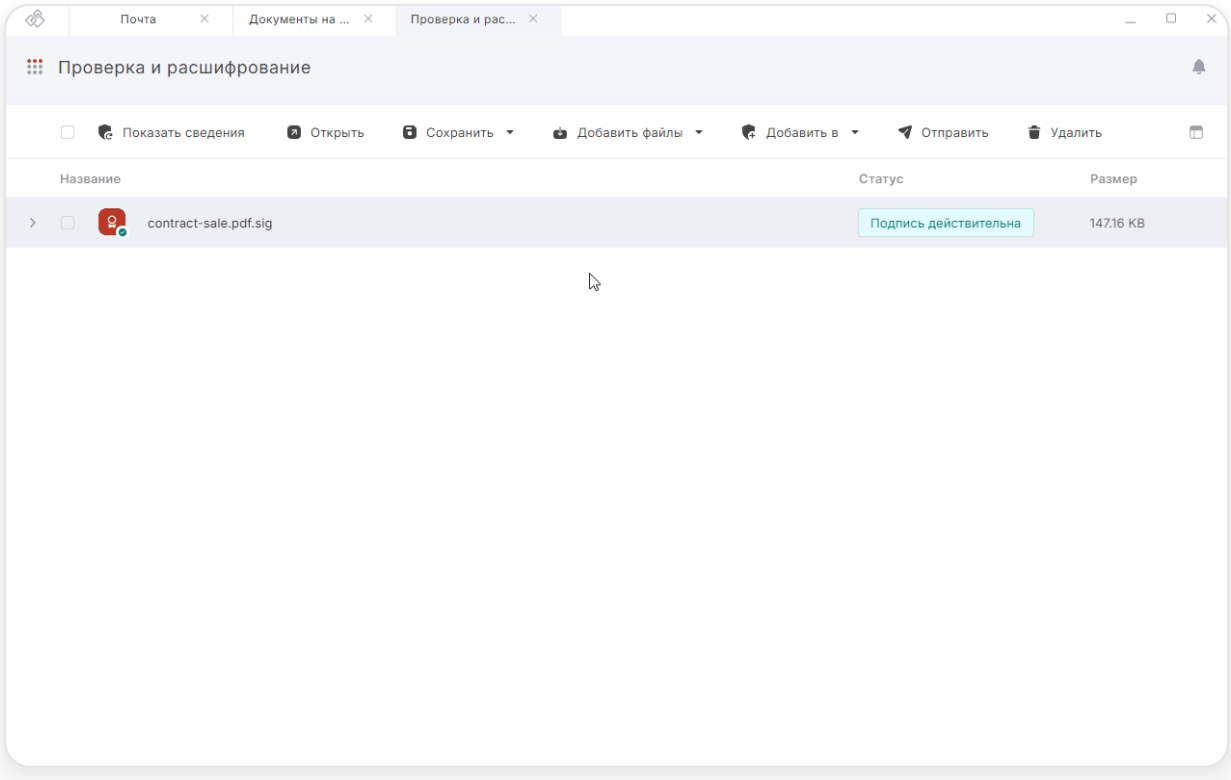
1. Перейдите в раздел **Почта**.
2. Откройте письмо.

3. Нажмите на кнопку **Скачать все**, размещенную над вложенными файлами.
4. Укажите путь для сохранения архива в окне файлового менеджера.

Открытие вложенного файла

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Дождитесь скачивания вложений, если у вас активна настройка **Получать только текст сообщений**.
4. Нажмите на название вложенного файла.
5. Файл откроется в программе, установленной по умолчанию.

> 💡 Подписанные и зашифрованные документы будут открыты в мастере **Проверка и расшифрование**.



Статичный кадр демонстрации. Открыть анимацию

Инструкции по теме

- Отправка подписанного и зашифрованного сообщения

- Отправка письма с уведомлениями о доставке и прочтении
- Добавление почтового аккаунта
- Создание контакта

Открыть статью на сайте

Проверка подписи письма

- Общие сведения
- Как проверить подпись письма
- Дополнительные действия

Общие сведения

> 💡 **С чего начать**: Чтобы оценить, готово ли ваше рабочее место для работы с защищенной почтой, воспользуйтесь Проверкой рабочего места.

Обозначение подписанных писем

В списке сообщений подписанные письма отмечаются специальными иконками в виде сертификата  .

При просмотре письма цвет иконок меняется в зависимости от статуса подписи:

Статус	Визуальное обозначение	Описание
Подпись действительная		Подпись прошла все проверки
Подпись недействительная		Обнаружены проблемы с подписью
Статус подписи неизвестен		Обнаружены проблемы с подписью. Возможно, отсутствует поддержка алгоритма сертификата подписи.

Распространенные проблемы

Причины, по которым подпись может быть недействительной:

Причина	Возможность исправления	Рекомендуемые действия
Срок действия сертификата подписи истек, либо сертификат отозван	❌ Невозможно исправить	Запросите новое письмо, подписанное действительным сертификатом
Письмо было изменено после подписания	❌ Невозможно исправить	Запросите новое подписанное письмо

Причина	Возможность исправления	Рекомендуемые действия
Нет доверия к сертификату (отсутствует корневой сертификат)	✅ Можно исправить	Импортируйте корневой сертификат удостоверяющего центра, выпустившего сертификат отправителя
Отсутствует актуальный список отзыва	✅ Можно исправить	Импортируйте актуальный список отзыва сертификатов (CRL)

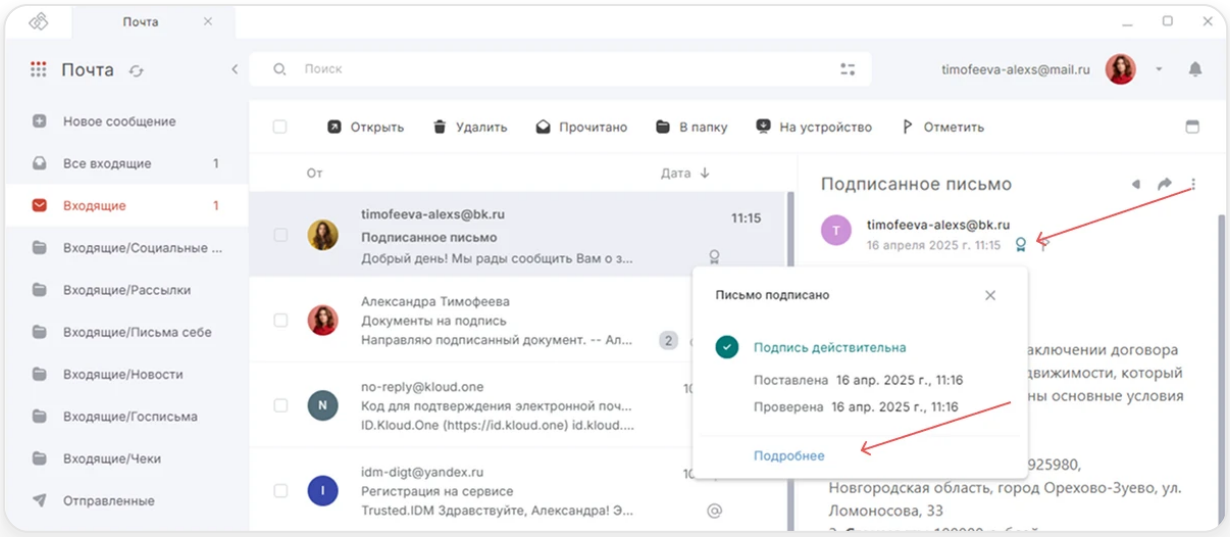
Как проверить подпись письма

> 💡 **Совет**: В расширенном поиске есть возможность установить фильтр для подписанных писем.

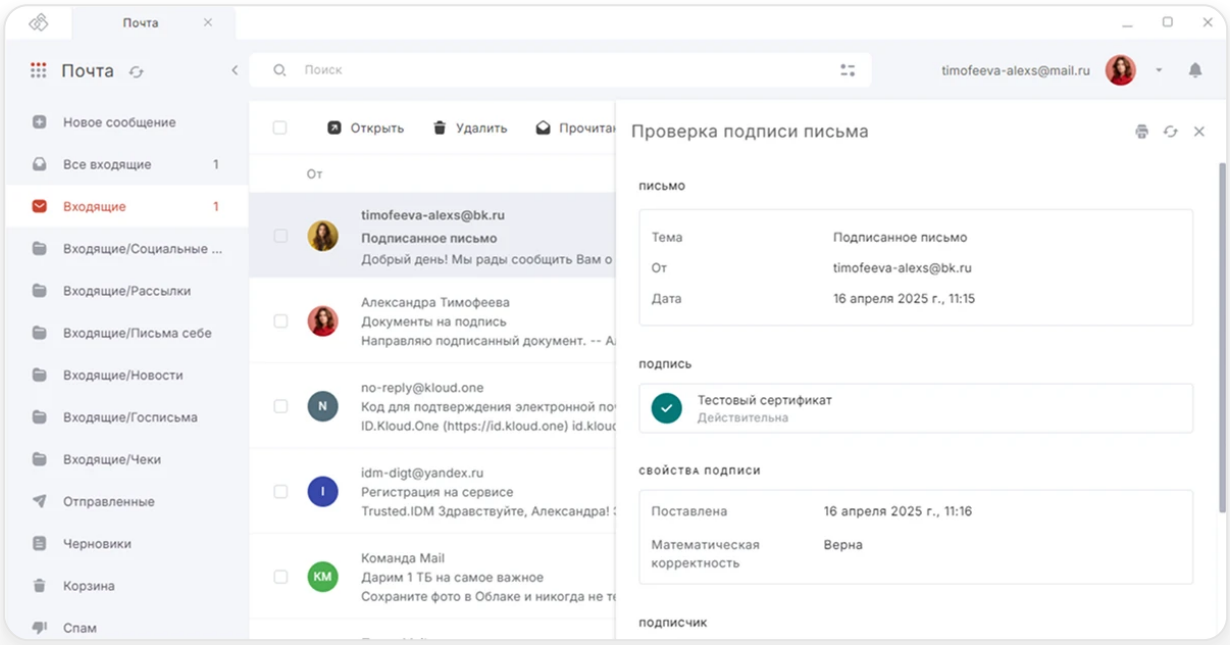
1. Перейдите в раздел **Почта**.
2. Откройте подписанное письмо.
3. В окне просмотра письма будет отображаться иконка .

   В зависимости от статуса подписи письма иконка будет иметь цвет:

   - зеленый цвет, если подпись письма действительная,
   - красный цвет, если подпись недействительная,
   - серый цвет, если статус подписи неизвестен.
4. Нажмите на иконку на панели с подписанным письмом в списке писем или в окне просмотра письма.
5. Откроется окно со статусом подписи, датой подписания и проверки.



Для просмотра детальной информации о подписи нажмите **Подробнее**.



Дополнительные действия

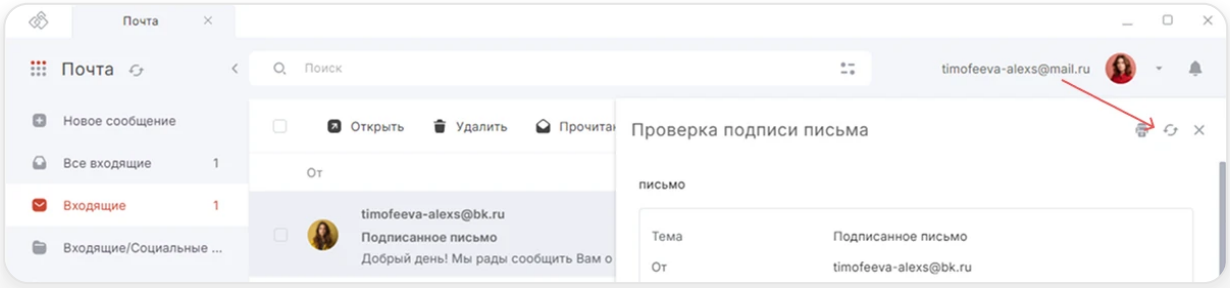
Обновление сведений о подписи письма

В некоторых случаях, например, при установке корневого или промежуточного сертификата, может потребоваться повторная проверка подписи письма.

Чтобы запустить повторную проверку подписи:

1. Выполните шаги из инструкции Проверка подписи письма.

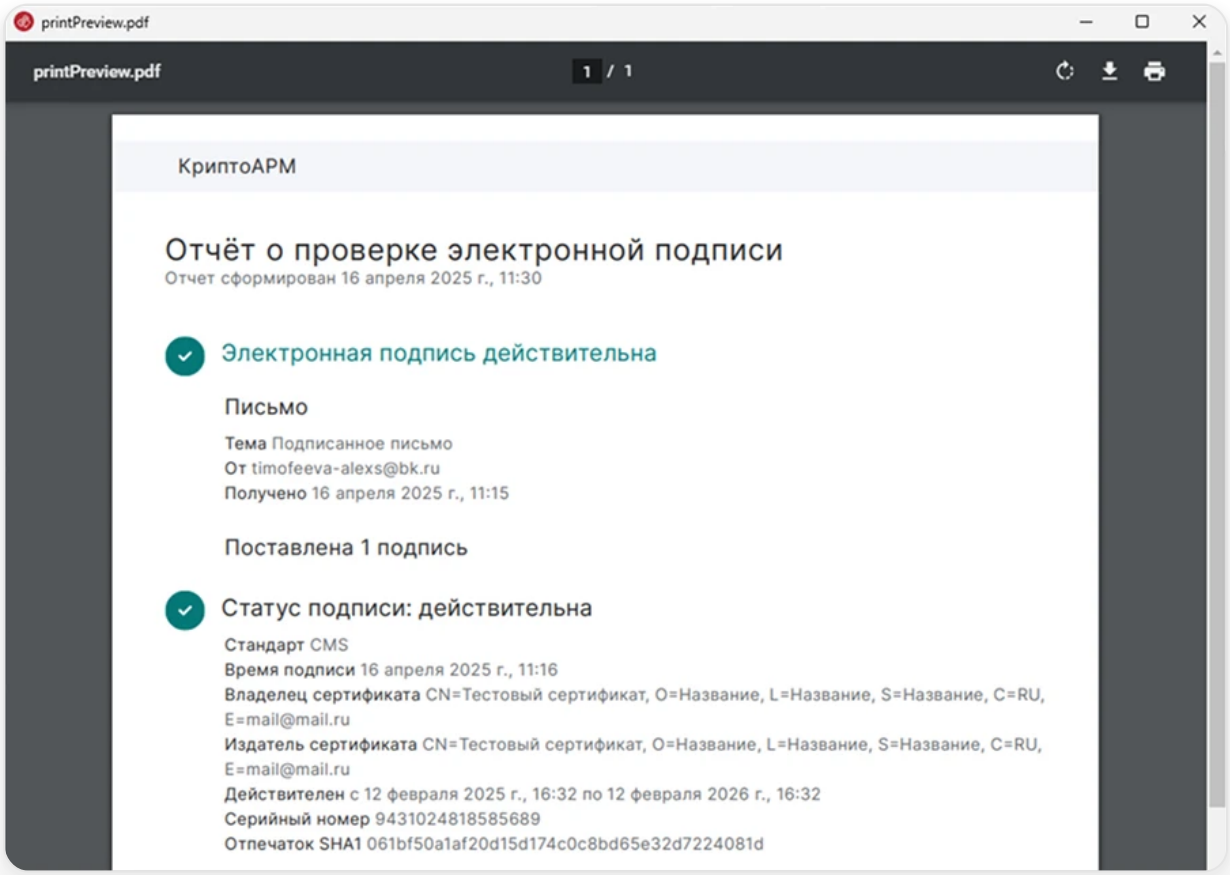
2. В окне с детальными сведениями о подписи нажмите на кнопку **Обновить** .



Сведения о подписи будут обновлены.

Печать сведений о подписи письма

1. Выполните шаги из инструкции Проверка подписи письма.
2. В окне с детальными сведениями о подписи нажмите на кнопку **Печать** .
3. Откроется окно с печатной формой отчета.

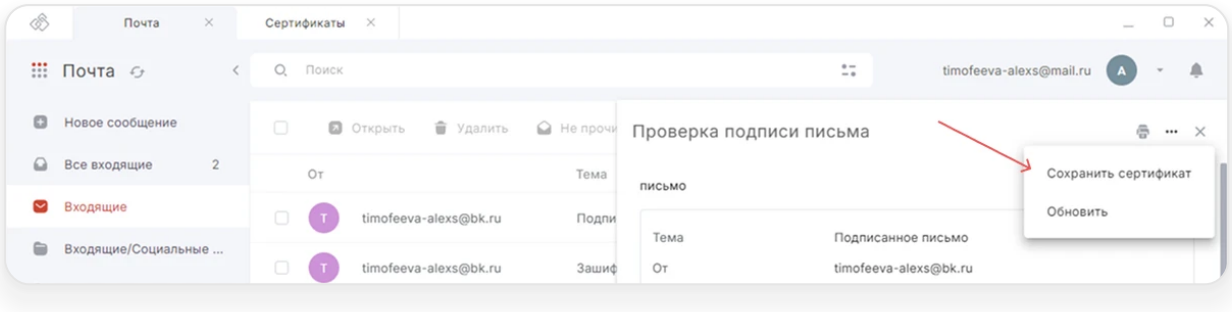


Отчет можно распечатать или скачать на устройство.

Сохранение сертификата подписи

Чтобы сохранить сертификат подписи в разделе **Сертификаты**:

1. Выполните шаги из инструкции Проверка подписи письма.
2. В окне с детальными сведениями о подписи нажмите на кнопку **Еще**.
3. В появившемся меню с действиями выберите действие **Сохранить сертификат**.



Сертификат подписи письма будет сохранен в хранилище **Сертификаты других пользователей** раздела **Сертификаты**.

Инструкции по теме

- Проверка рабочего места
- Отправка подписанного и зашифрованного сообщения
- Действия с письмами
- Установка личного сертификата
- Установка корневого и промежуточного сертификата

Открыть статью на сайте

Расшифрование письма

- Как расшифровать письмо
- Возможные ошибки

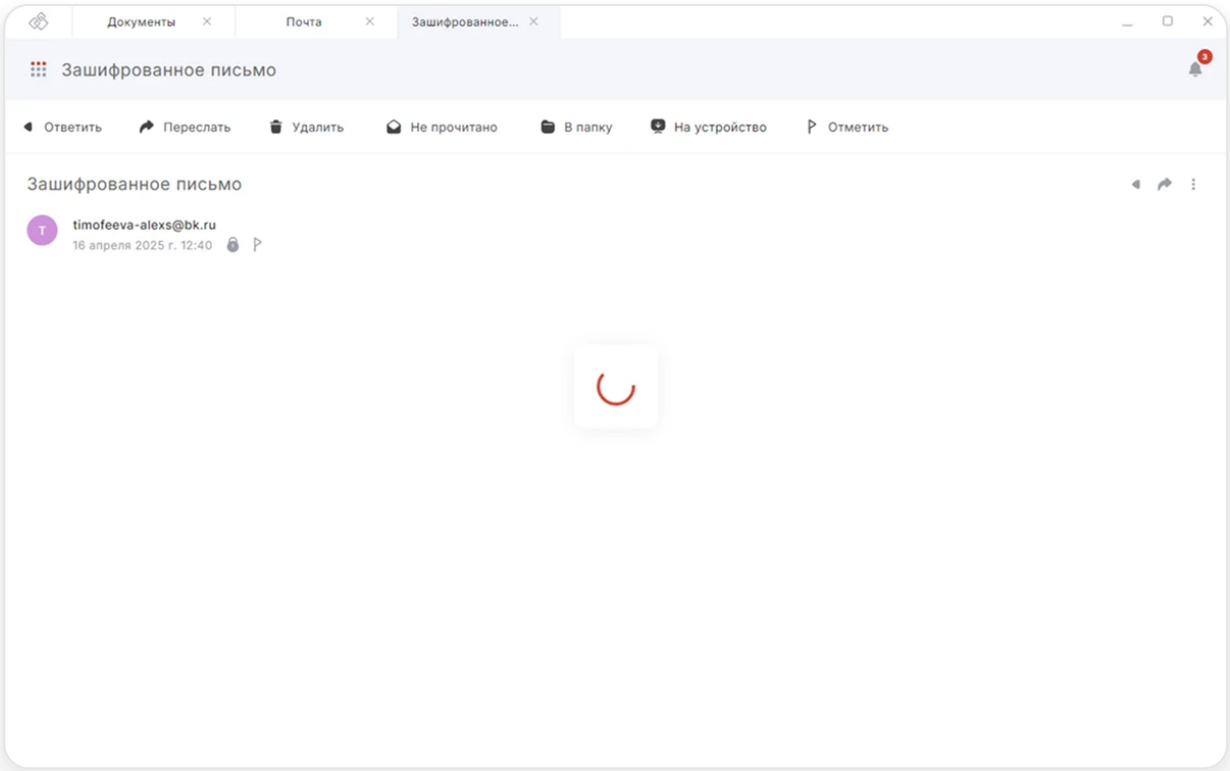
> 💡 **С чего начать**: Чтобы оценить, готово ли ваше рабочее место для работы с защищенной почтой, воспользуйтесь Проверкой рабочего места.

Как расшифровать письмо

> 💡 В списке сообщений зашифрованные письма обозначаются специальными значками в виде замка 🔒.

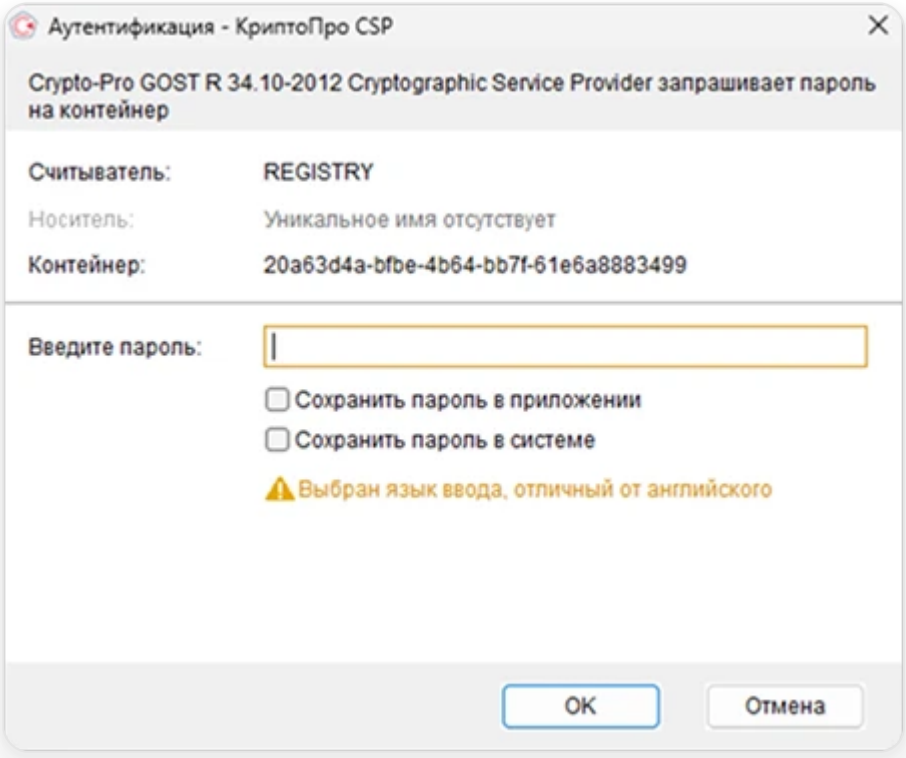
1. Перейдите в раздел **Почта**.
2. Откройте письмо, которое необходимо расшифровать.

> 💡 **Совет**: В расширенном поиске есть возможность установить фильтр для зашифрованных писем.



3. При открытии письмо расшифровывается автоматически, если найден сертификат расшифрования и сохранен пароль к закрытому ключу. Если пароль не был сохранён, вам нужно будет ввести его.

   Пример окна для криптопровадера КриптоПро CSP:



При необходимости вы можете повторить расшифрование. Для этого на форме просмотра письма вызовите меню действий по кнопке **Еще** ⋮ и выберите действие **Расшифровать**.

Возможные ошибки

При возникновении ошибок вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Рекомендуемые действия
Сообщение не расшифровано	Возможно, в хранилище "Личные" не обнаружен сертификат для расшифрования. Установите сертификат и повторите попытку расшифрования.
Сообщение не расшифровано (Для писем, зашифрованных в адрес сертификата с алгоритмами ГОСТ)	Возможно, отсутствует криптопровайдер, поддерживающий алгоритм шифрования. Установите криптопровайдер КриптоПро CSP и перезапустите приложение КриптоАРМ
Отсутствует действующая лицензия КриптоАРМ	1. Приобретите или продлите лицензию КриптоАРМ 2. Активируйте лицензию в настройках программы
Отсутствует действующая лицензия КриптоПро CSP	Установите лицензию КриптоПро CSP

Инструкции по теме

- Проверка рабочего места
- Отправка подписанного и зашифрованного сообщения
- Действия с письмами
- Установка личного сертификата

Открыть статью на сайте

Письма с уведомлениями

- Исходящие письма с запросом уведомлений
- Входящие письма с запросом подтверждения прочтения

Исходящие письма с запросом уведомлений

Идентификация писем

В списке сообщений отправленные письма с уведомлениями отмечаются специальными иконками в виде галочки:

-  для писем с уведомлениями о доставке,
-  для писем с уведомлениями о прочтении.

При получении подтверждения о доставке и прочтении письма цвет значков меняется:

Статус	Визуальное обозначение
Прочитано всеми/Доставлено	
Прочитано не всеми получателями/Не доставлено	
Доставлено всем	
Доставлено не всем получателям	

Как узнать доставлено ли письмо

При получении письма на сервер получателя вам придет автоматическое письмо-уведомление.

Уведомление о доставке подтверждает доставку сообщения, но не гарантирует, что оно было просмотрено или прочитано.

> 💡 **Совет**: Для удобной организации почты вы можете настроить автоматическое перемещение служебных уведомлений в специальную папку **Уведомления**. Подробнее о специальных папках читайте в инструкции Настройки подключения.

Статус доставки можно также просмотреть в папке **Отправленные**:

1. Перейдите в раздел **Почта**.
2. Откройте папку **Отправленные**.
3. Найдите нужное письмо в списке.
4. Нажмите на иконку ✓, размещенную на панели с письмом в списке писем или в окне просмотра письма.
5. Откроется окно со сведениями о доставке.

Как узнать прочитано ли письмо

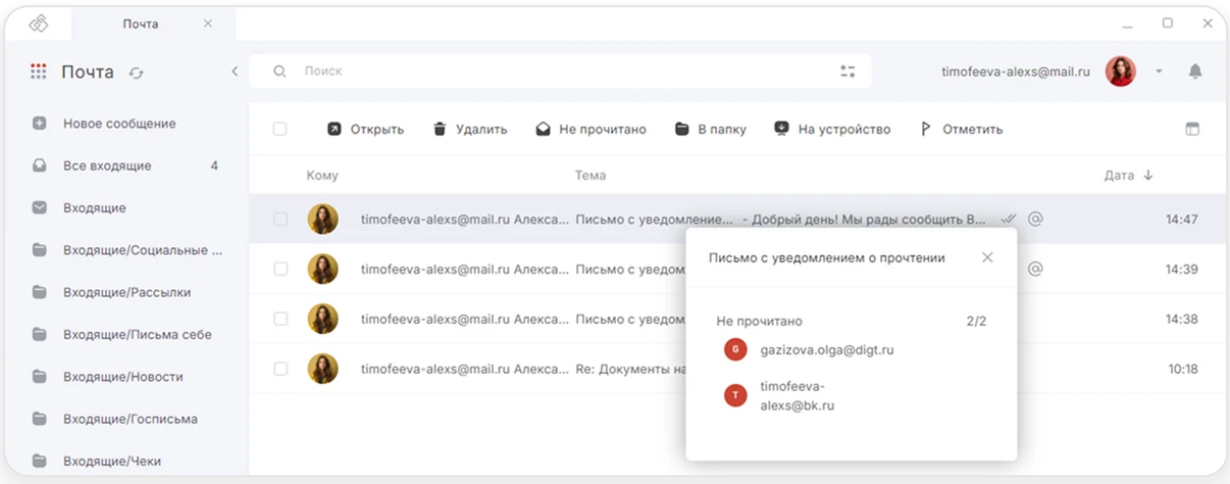
Чтобы вы могли получить подтверждение прочтения, получатель вашего письма, должен будет сначала его отправить. Подтверждение будет направлено в виде отдельного письма-уведомления, в котором будет указана дата и время, когда ваше сообщение было открыто.

Подтверждение не гарантирует фактическое прочтение письма получателем. Принцип работы с подтверждениями зависит от используемой почтовой системы.

> 💡 **Совет**: Для удобной организации почты вы можете настроить автоматическое перемещение служебных уведомлений в специальную папку **Уведомления**. Подробнее о специальных папках читайте в инструкции Настройки подключения.

Статус подтверждений можно также просмотреть в папке **Отправленные**:

1. Перейдите в раздел **Почта**.
2. Откройте папку **Отправленные**.
3. Найдите нужное письмо в списке.
4. Нажмите на иконку ✓✓, размещенную на панели с письмом в списке писем или в окне просмотра письма.
5. Откроется окно со сведениями о прочтении.



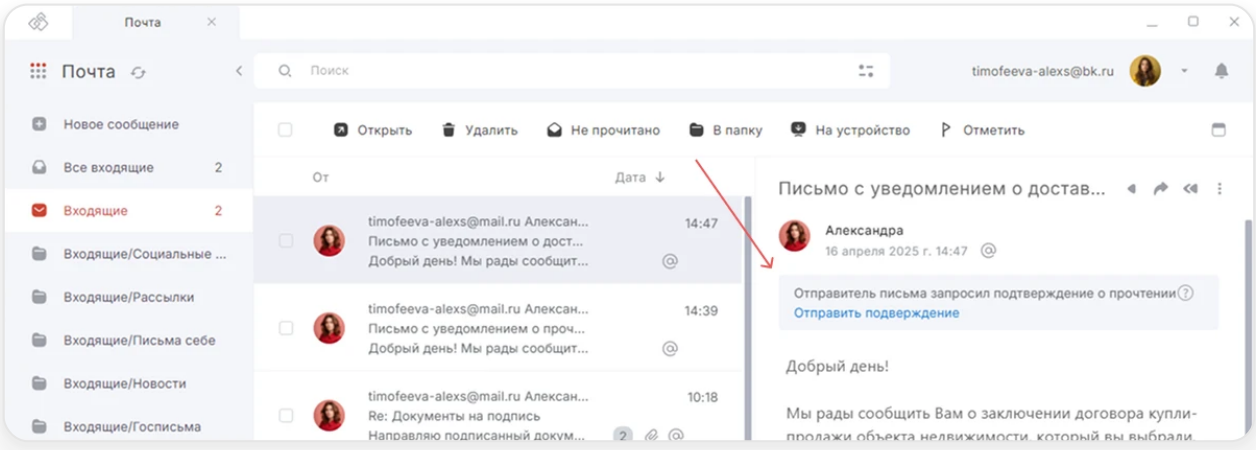
Основные причины отсутствия подтверждений

Функция подтверждений прочтения поддерживается большинством почтовых систем, однако существуют ситуации, когда вы можете их не получить:

- **Групповые рассылки.** При отправке сообщений через списки рассылки или групповые псевдонимы подтверждения могут не приходить.
- **Ограничения администратора.** Ваш системный администратор может ограничить отправку подтверждений только для сотрудников организации или определенных внешних получателей.
- **Тип почтового клиента:**
  - Использование программ с протоколом **POP**, которые синхронизируются только по запросу,
  - Работа с **Google Workspace Sync**,
  - Использование почтовых клиентов **IMAP**, блокирующих подтверждения.

Входящие письма с запросом подтверждения прочтения

Если в настройках вашего почтового аккаунта включена функция "Каждый раз спрашивать, следует ли отправлять уведомление о прочтении", то каждое входящее письмо с запросом на подтверждение получения будет содержать специальный информер.



> 💡 **Совет**: Вы можете скрыть запрос уведомлений о прочтении из интерфейса. Кроме того, можно настроить автоматическую отправку уведомлений о прочтении писем сразу после их получения. Подробнее читайте в инструкции Общие настройки.

Отправка подтверждения о прочтении

1. Перейдите в раздел **Почта**.
2. Откройте письмо, прочтение которого необходимо подтвердить.
3. Нажмите **Отправить подтверждение** в информере.
4. Приложение автоматически сформирует и отправит ответ.

После отправки подтверждения информер будет скрыт из письма.

Инструкции по теме

- Проверка рабочего места
- Отправка подписанного и зашифрованного сообщения
- Действия с письмами
- Добавление почтового аккаунта
- Создание контакта

Открыть статью на сайте

Черновики писем

- Создание черновика
- Продолжение работы с черновиком

Создание черновика

Во время написания письма вы можете закрыть черновик и вернуться к нему позже.

Чтобы создать черновик:

1. Перейдите в раздел **Почта**.
2. Нажмите на кнопку **Новое сообщение** в меню слева.
3. Откроется вкладка с новым письмом.
4. Заполните необходимые поля:
    - Укажите получателей (можно оставить пустым),
    - Напишите тему и текст письма,
    - При необходимости добавьте вложения.
5. Закройте вкладку с письмом. Черновик будет сохранен автоматически.

Сохраненный черновик можно найти в папке **Черновики**.

> 💡 Черновик сохраняется до тех пор, пока не будет отправлен или удален.

Продолжение работы с черновиком

Чтобы продолжить работу с черновиком:

1. Перейдите в раздел **Почта**.
2. Откройте папку **Черновики** в меню слева.
3. Откройте черновик одним из способов:
    - Выделите черновик в списке писем и нажмите кнопку **Открыть** на панели действий.
    - Дважды кликните по панели с черновиком.
4. Откроется новая вкладка с черновиком.

Инструкции по теме

- Проверка рабочего места
- Отправка подписанного и зашифрованного сообщения
- Действия с письмами
- Добавление почтового аккаунта
- Создание контакта

Открыть статью на сайте

Удаление и восстановление письма

- Как удалить письма
- Очистка корзины
- Восстановление письма

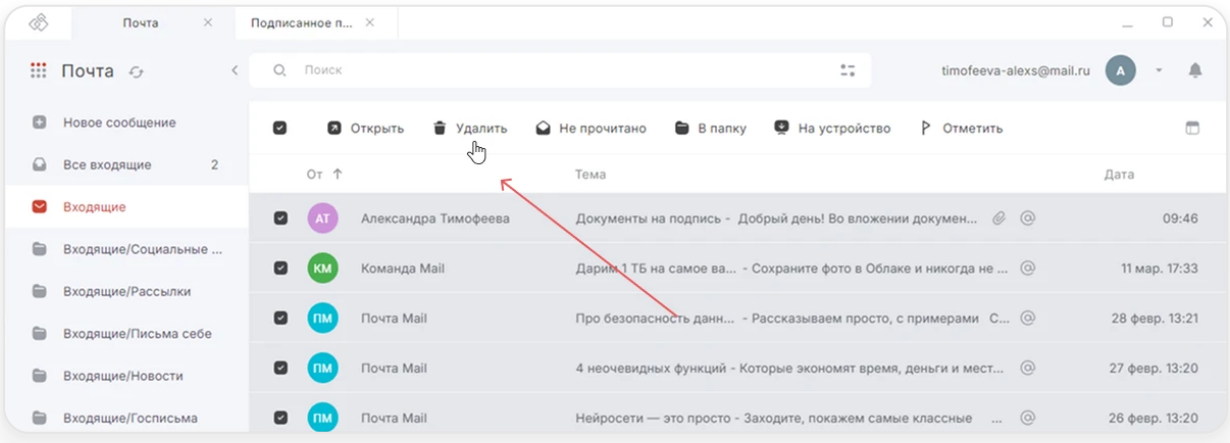
Как удалить письма

> ⚠️ **Примечание**: Когда вы удаляете письма из папки **Сохранённые письма**, они удаляются безвозвратно.

1. Удаление в списке писем

Чтобы удалить одно или несколько писем в списке писем:

1. Перейдите в раздел **Почта**.
2. Выделите одно или несколько писем в списке.
3. Нажмите на кнопку **Удалить** на панели действий.
4. Письма будут перемещены в папку **Корзина**.

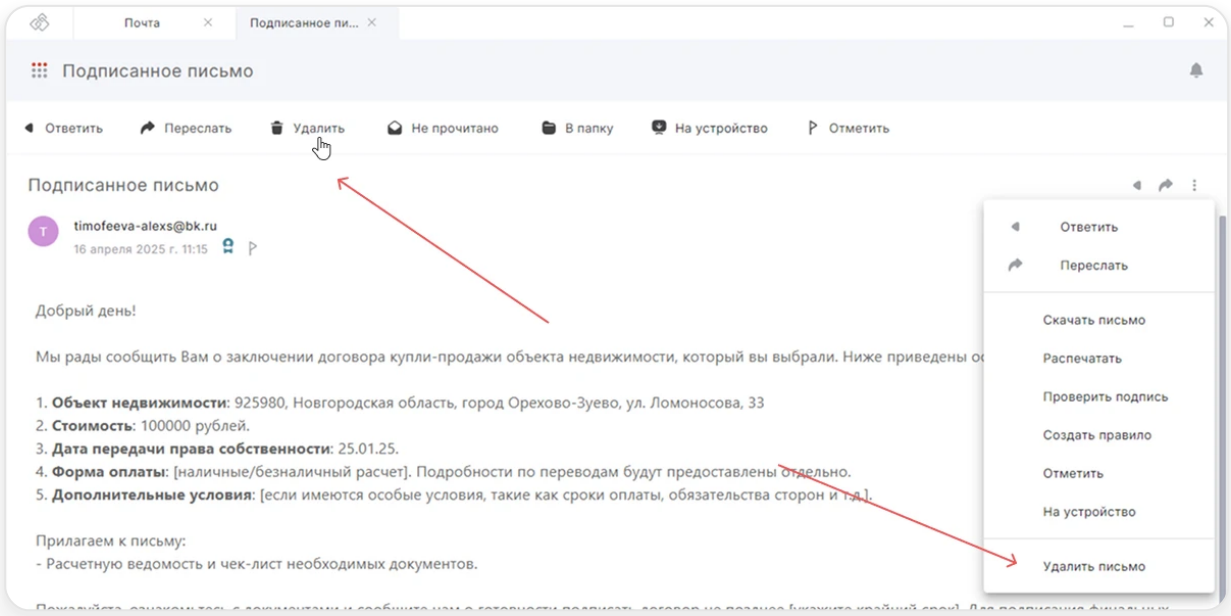


2. Удаление при чтении письма

Чтобы удалить письмо на вкладке просмотра:

1. Перейдите в раздел **Почта**.
2. Откройте письмо.

3. Выполните действие одним из способов:
   - Нажмите на кнопку **Удалить** на панели действий.
   - Вызовите меню действий по клику на кнопку **Еще** ⋮ и выберите действие **Удалить**.
4. Письмо будет перемещено в папку **Корзина**.

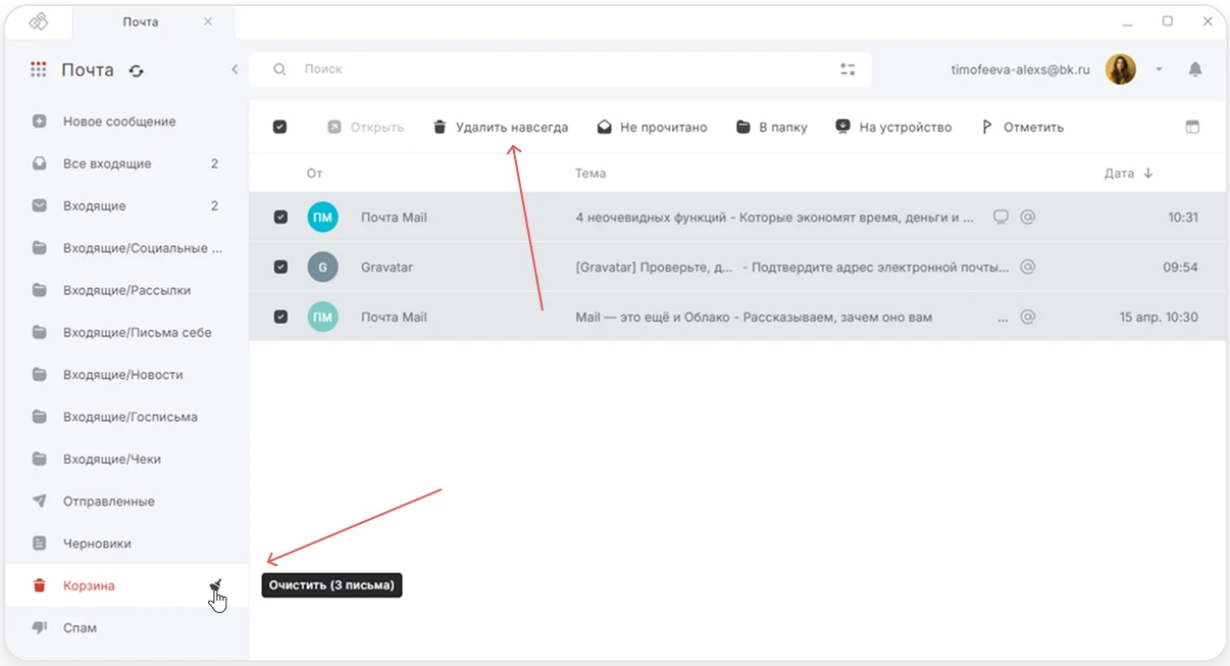


3. Удаление письма из цепочки

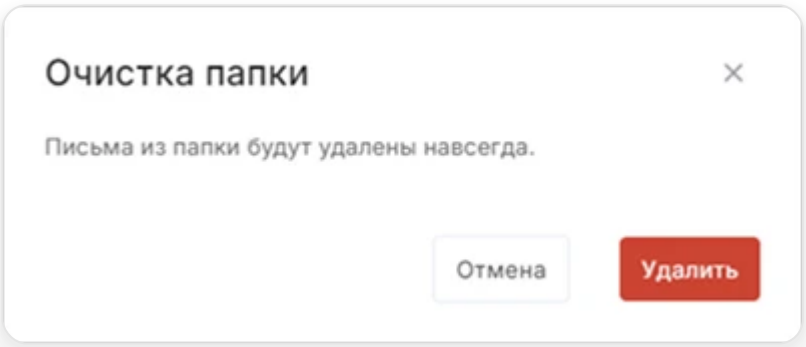
1. Перейдите в раздел **Почта**.
2. Откройте цепочку писем.
3. Вызовите меню действий по клику на кнопку **Еще** ⋮ для письма, которое необходимо удалить.
4. Выберите действие **Удалить**.
5. Выбранное письмо будет перемещено в папку **Корзина**.

Очистка корзины

1. Перейдите в раздел **Почта**.
2. Откройте папку **Корзина**.
3. Выполните действие одним из способов:
   - Установите флажки напротив писем, которые хотите удалить навсегда и нажмите **Удалить навсегда**,
   - Нажмите кнопку **Очистить**, размещенную в боковом меню слева.



4. Подтвердите действие в модальном окне.



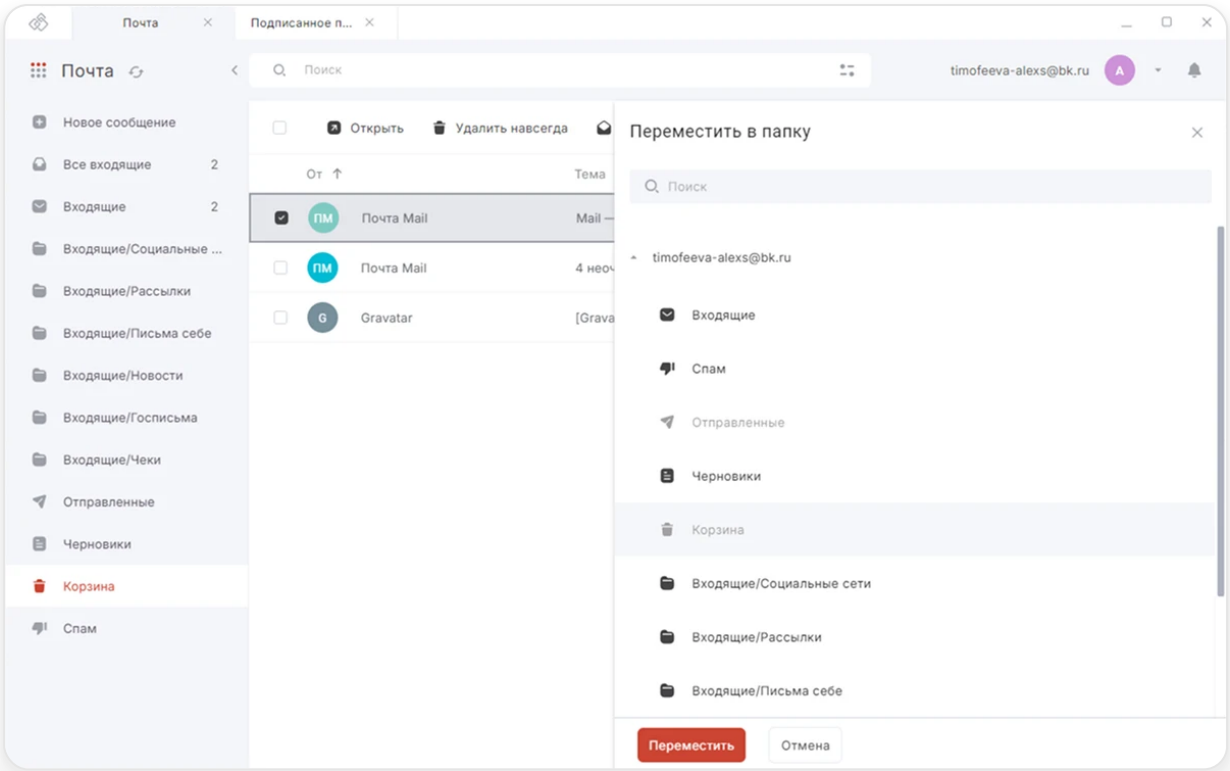
Восстановление письма

Если вы переместили письмо в папку **Корзина**, его можно восстановить.

Чтобы восстановить письма, удаленные в папку **Корзина**:

1. Перейдите в раздел **Почта**.
2. Откройте папку **Корзина**.
3. Установите флажки напротив писем, которые хотите восстановить.
4. Нажмите на кнопку **В папку** на панели действий.

5. Откроется окно со списком папок.



6. Выберите нужную папку.
7. Нажмите **Переместить**.

Инструкции по теме

- Проверка рабочего места
- Отправка подписанного и зашифрованного сообщения
- Действия с письмами
- Добавление почтового аккаунта
- Создание контакта

Открыть статью на сайте

Автоматическая сортировка писем

- Критерии сортировки
- Доступные действия
- Создание правила сортировки
- Управление правилами

> 📌 **Сортировка писем** позволяет автоматически организовать входящую почту по заданным правилам.

Критерии сортировки

Вы можете создавать правила на основе следующих параметров:

Критерий	Доступные условия	Описание	Пример использования
Отправитель	содержит, не содержит, совпадает с, не совпадает с	Фильтрация по адресу/имени отправителя	Все письма от *@domain.com
Получатель	содержит, не содержит, совпадает с, не совпадает с	Фильтрация по адресу получателя	Письма для support@company.com
Тема письма	содержит, не содержит, совпадает с, не совпадает с	Фильтрация по словам в теме	Письма с темой "Счёт" или "Invoice"
Содержание письма	содержит, не содержит, совпадает с, не совпадает с	Фильтрация по ключевым словам в теле письма	Письма со словом "договор"
Название вложения	содержит, не содержит, совпадает с, не совпадает с	Фильтрация по имени файлов вложений	Письма с файлом "report.pdf"
Дата получения	До, После	Фильтрация по дате отправки/получения	Письма после 01.01.2023
Статус	Подписанные, Зашифрованные, Содержит вложение	Фильтрация по специальным статусам	Все подписанные письма
Размер	Больше, Меньше	Фильтрация по размеру письма	Письма больше 10 МБ

Критерий	Доступные условия	Описание	Пример использования
Все входящие	-	Общее правило для всех писем	Применение действия ко всей входящей почте

Доступные действия

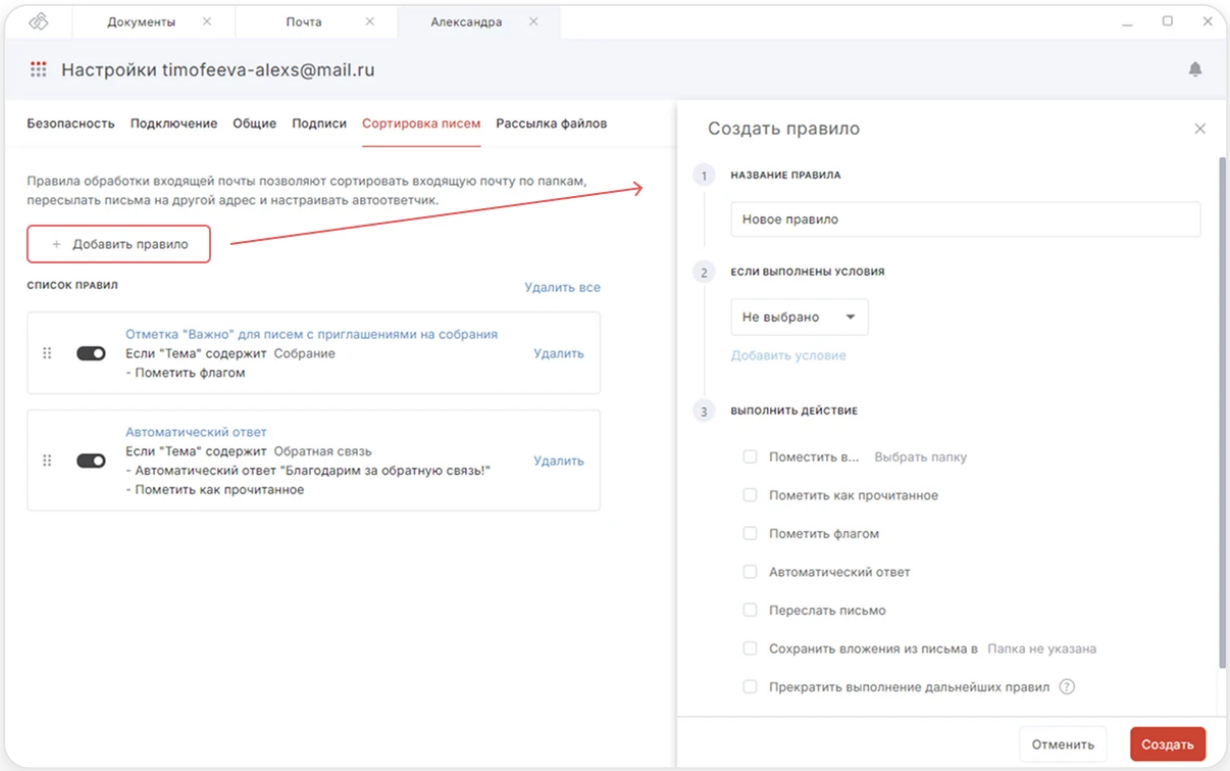
Для писем, соответствующих заданным условиям, можно настроить:

Действие	Описание
Перемещение в папку	Автоматическое перемещение в указанную папку
Пометка как прочитанного	Изменение статуса письма с непрочитанного на прочитанное
Автоматический ответ	Отправка шаблонного ответа. Настраивается текст и получатели.
Пересылка	Перенаправление письма другому адресату. Можно указать несколько получателей.
Сохранение вложений	Автоматическое скачивание файлов. Указывается папка для сохранения.
Прекращение обработки	Остановка выполнения последующих правил. Используется для приоритизации правил.
Применение к существующим	Применение правила к уже полученным письмам в папке «Входящие»

Создание правила сортировки

1. Стандартный способ

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Сортировка писем**.
3. Нажмите **Добавить правило**.
4. Откроется окно **Создать правило**.



5. Укажите название правила.

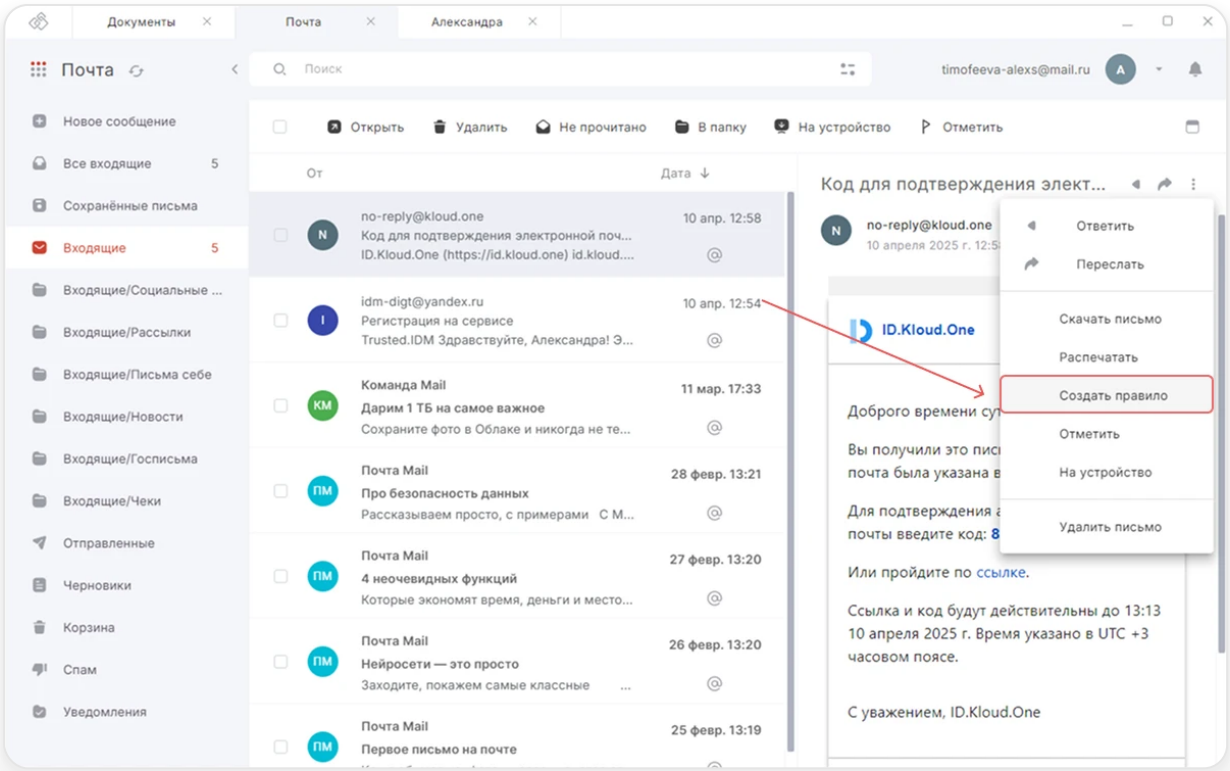
6. Добавьте одно или несколько условий.
7. Укажите действие, которое необходимо выполнить с письмом.
8. Нажмите **Создать**.

---

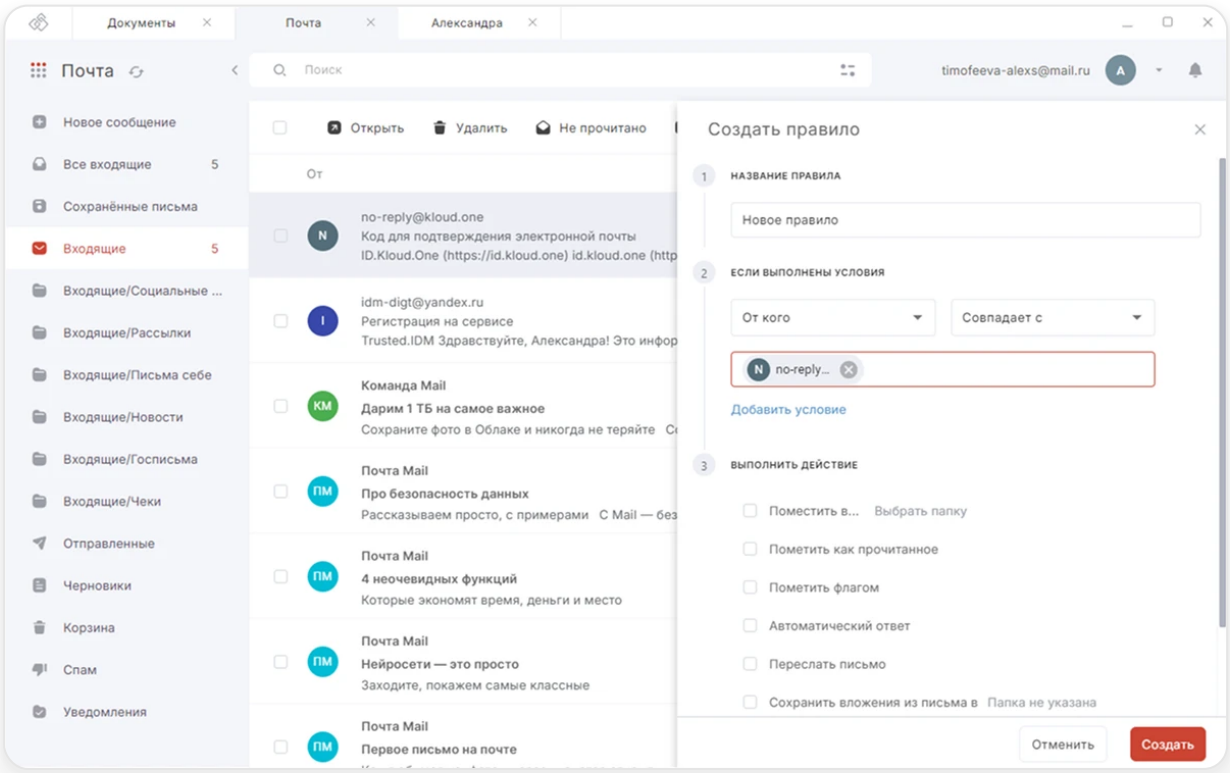
2. Создание из письма

1. Перейдите в раздел **Почта**.
2. Откройте письмо, для которого необходимо создать правило.
3. Вызовите меню действий с вложением по кнопке **Еще**.

4. Выберите **Создать правило**.



5. Откроется окно **Создать правило**.



6. Добавьте одно или несколько условий.

7. Укажите действие, которое необходимо выполнить с письмом.

8. Нажмите **Создать**.

Управление правилами

1. Редактирование правила сортировки

Чтобы отредактировать правило сортировки:

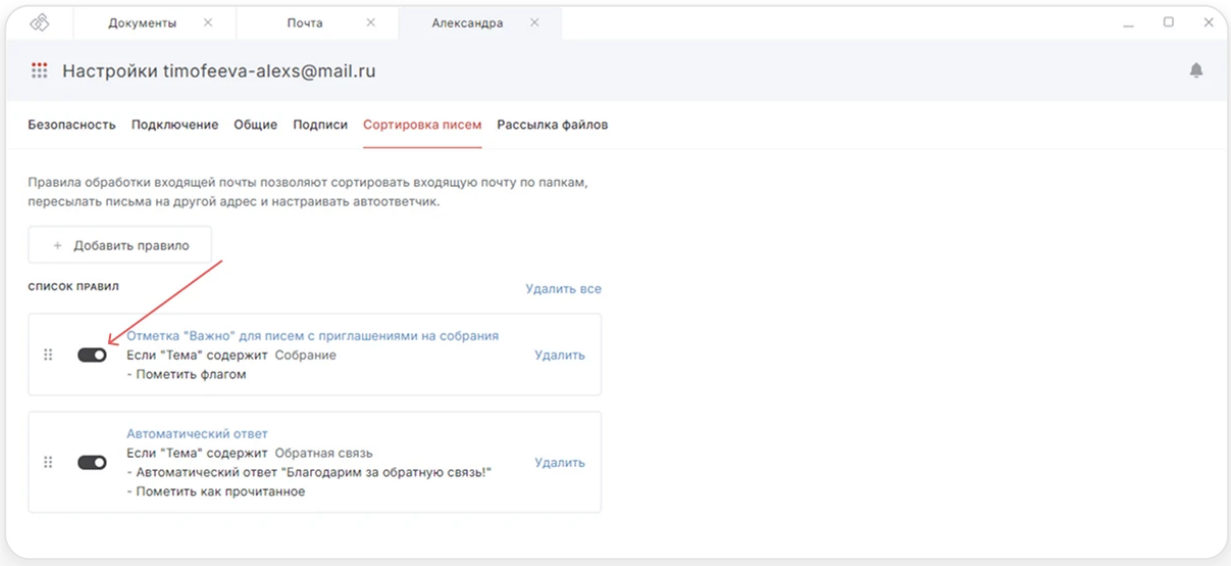
1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Сортировка писем**.
3. Нажмите на название правила, настройки которого необходимо отредактировать.
4. В открывшемся окне внесите изменения в настройки и нажмите **Сохранить**.

2. Изменение активности правила сортировки

Доступна временная активация или деактивация правила без его удаления.

Чтобы включить или отключить правило:

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Сортировка писем**.
3. Включите или выключите переключатель на панели с правилом в списке.



Изменения применяются автоматически без дополнительного подтверждения.

3. Изменение приоритета выполнения правил

Приоритет выполнения правил можно настроить, изменив порядок их отображения.

Правила выполняются сверху вниз. Письмо, обработанное одним правилом, может быть передано следующему, если не установлено действие «Прекратить обработку».

Чтобы поменять порядок правил:

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Сортировка писем**.
3. Наведите курсор мыши на кнопку ⠿, размещенную на панели с правилом. Удерживая левую кнопку мыши на кнопке, переместите правило в необходимое место в списке.

Изменения применяются автоматически без дополнительного подтверждения.

4. Удаление правил

Удаление правила

Чтобы удалить правило:

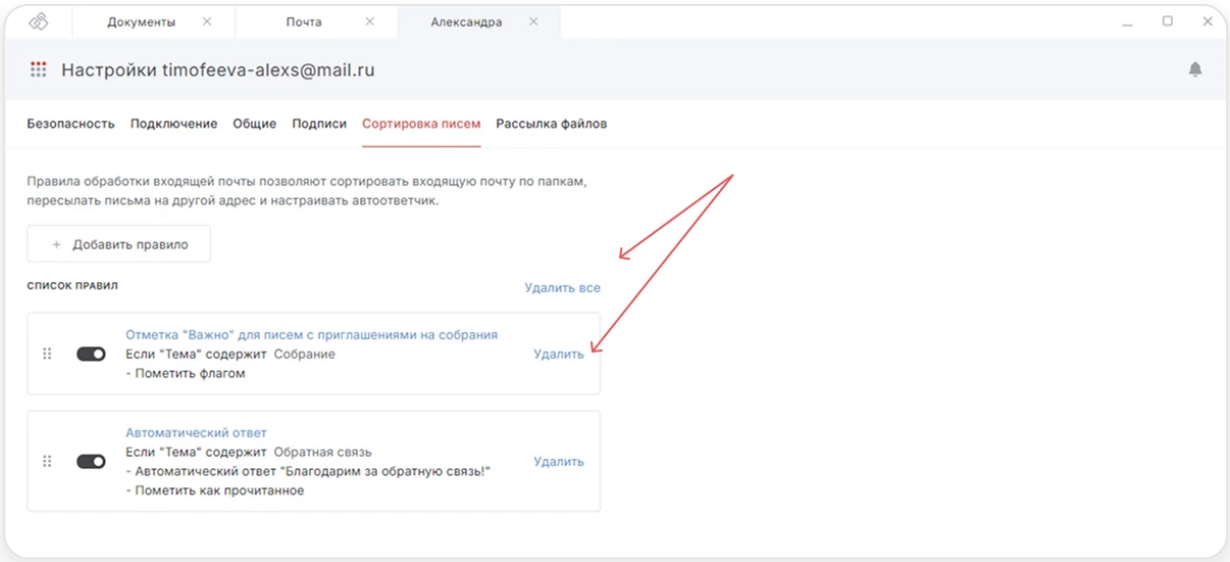
1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Сортировка писем**.
3. Нажмите на кнопку **Удалить**, размещенную на панели с правилом.
4. Подтвердите действие в модальном окне.

Групповое удаление

> 🚨 **Внимание!** Это удалит ВСЕ правила сортировки для этого аккаунта. Действие необратимо.

Чтобы удалить все правила:

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Сортировка писем**.
3. Нажмите на кнопку **Удалить все**, размещенную над списком правил.
4. Подтвердите действие в модальном окне.



Инструкции по теме

- Проверка рабочего места
- Отправка подписанного и зашифрованного сообщения
- Действия с письмами
- Добавление почтового аккаунта
- Создание контакта

Открыть статью на сайте

Поиск писем

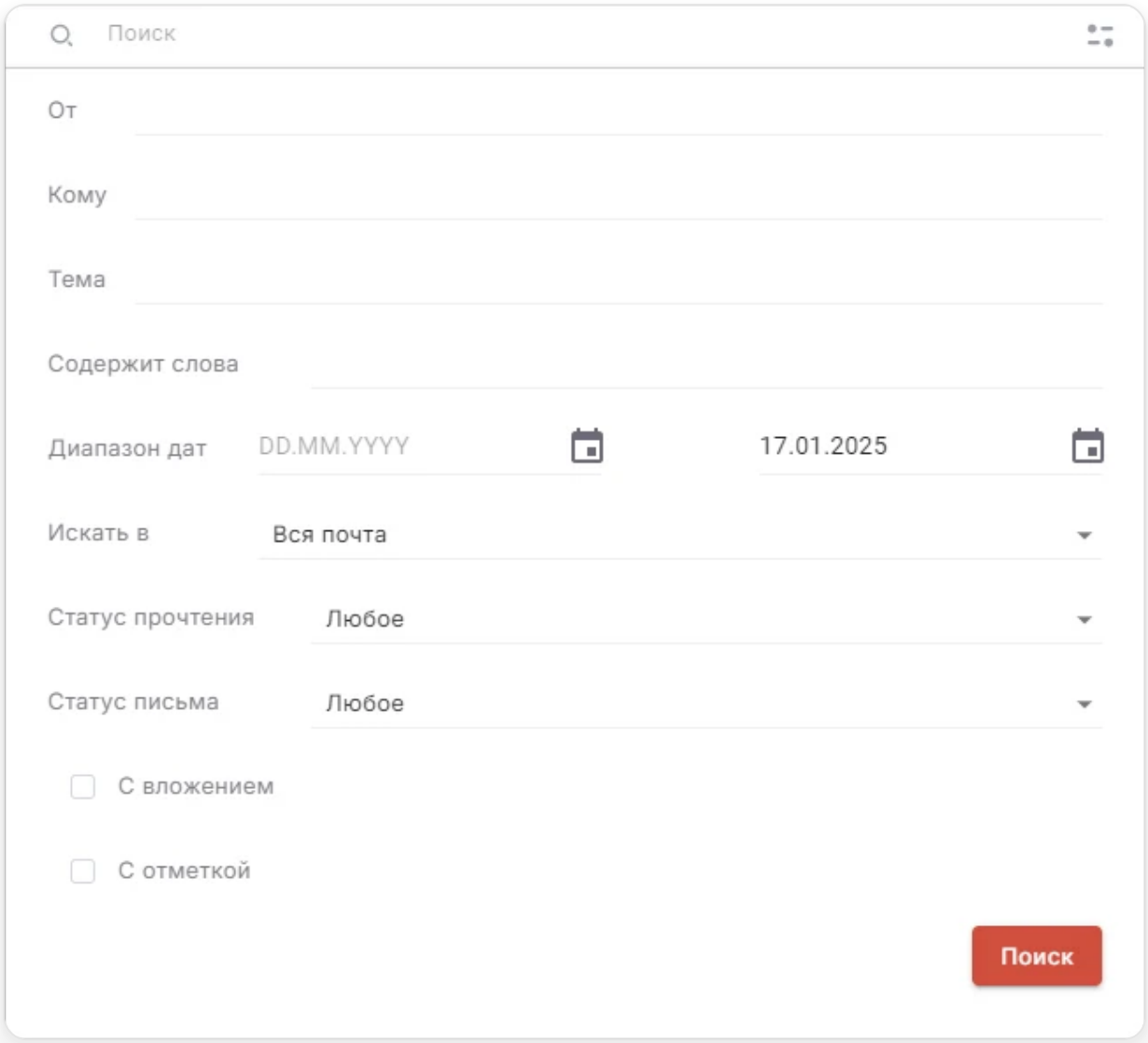
- Базовый поиск
- Расширенный поиск
- Управление результатами поиска

Базовый поиск

1. Перейдите в раздел **Почта**.
2. Введите в поисковой строке:
    - Имя отправителя;
    - Имя получателя;
    - Тему;
    - Текст содержания.
3. Нажмите **Enter**.

Расширенный поиск

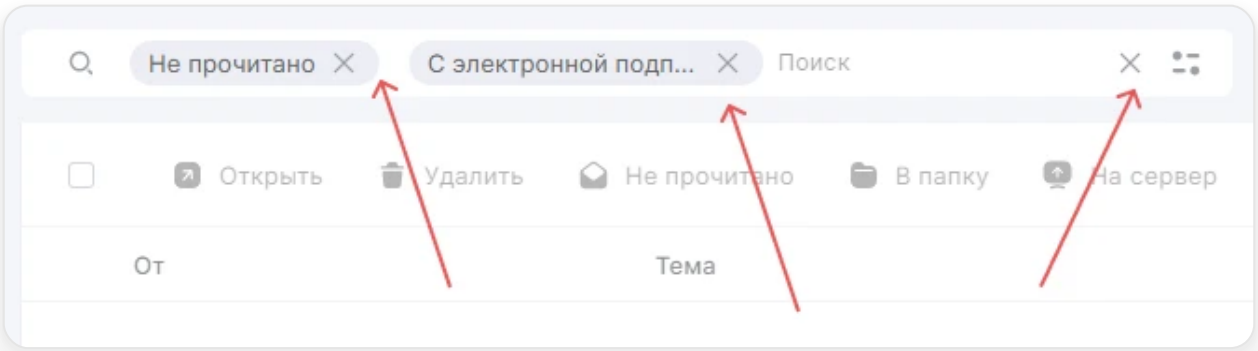
1. Перейдите в раздел **Почта**.
2. В строке поиска нажмите на иконку **Открыть фильтр** .
3. Откроется окно с фильтрами:
    - по имени отправителя;
    - по имени получателя;
    - по теме письма;
    - по содержанию слов в письме;
    - по диапазону дат;
    - относительно папки: **Вся почта**, **Входящие**, **Отправленные**, **Черновики**, **Корзина** и т. д.;
    - по статусу прочтения: **Любое**, **Прочитано**, **Не прочитано**;
    - по статусу письма: **Любое**, **Простое письмо**, **С электронной подписью**, **Зашифрованное**;
    - по параметру **С вложением**;
    - по параметру **С отметкой**.



4. Настройте параметры поиска.
5. Нажмите на кнопку **Поиск**.

Управление результатами поиска

- Для отмены фильтрации необходимо нажать на кнопку **Отмена** на чипсете с фильтром.
- Для быстрого доступа к истории поисков используйте выпадающий список в поисковой строке.



Инструкции по теме

- Проверка рабочего места
- Отправка подписанного и зашифрованного сообщения
- Действия с письмами
- Добавление почтового аккаунта
- Создание контакта

Открыть статью на сайте

Автоматическая рассылка файлов

- Создание рассылки файлов
- Управление рассылками

> 📌 **Рассылка файлов** — это инструмент, который позволяет настроить автоматическую отправку файлов в виде почтовых сообщений. Укажите папки, из которых будут забраны файлы, задайте параметры, необходимые для формирования письма и запустите рассылку.

Создание рассылки файлов

1. Откройте настройки почтового аккаунта.

   > 🔍 Как открыть настройки читайте в инструкции.

2. Перейдите на вкладку **Рассылка файлов**.

3. Нажмите **Добавить рассылку**.
4. Откроется окно **Создать рассылку**.
5. Укажите название рассылки.

6. Выберите папки для сканирования с устройства, из которых будут взяты файлы для рассылки.

   > ⚠️ **Примечание**: В рассылку попадут файлы только из корневой папки.

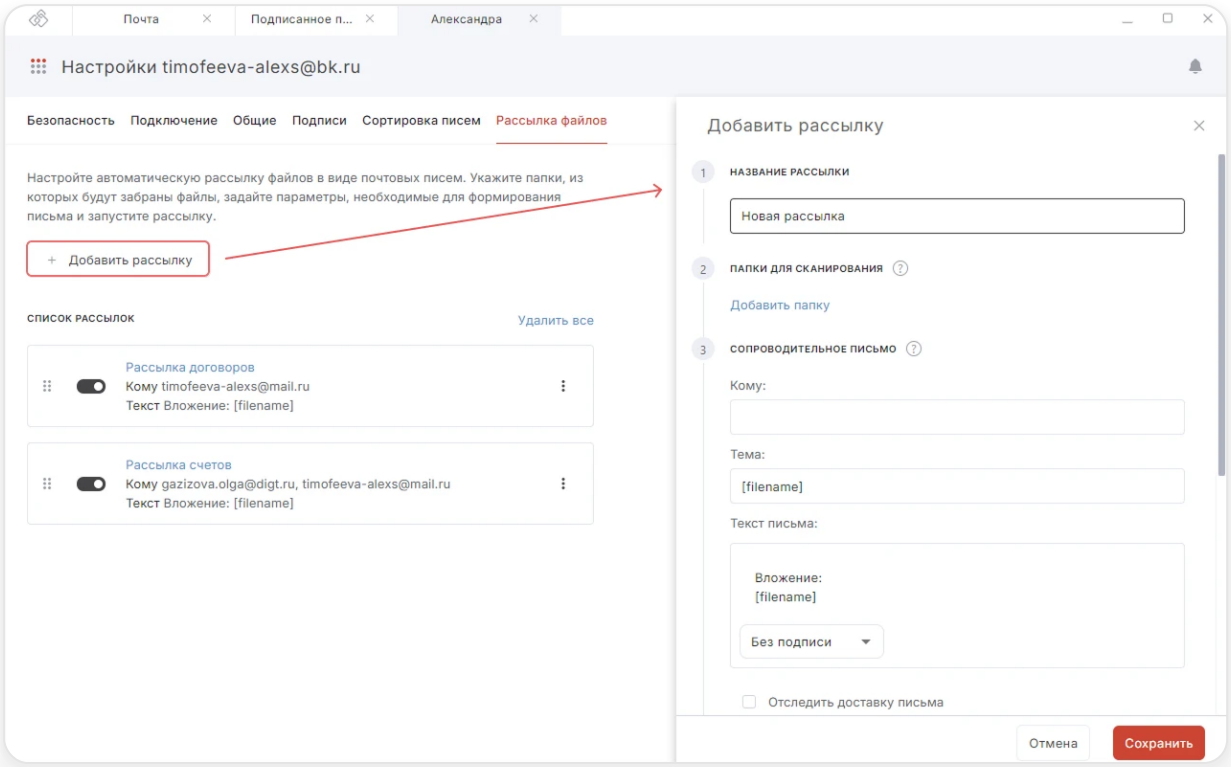
7. Добавьте текст сопроводительного письма.

   > 💡 **Совет**: В теме и тексте письма можно использовать константы: `[filename]` - имя файла, `[date]` - дата отправки письма, `[datetime]` дата и время отправки письма.

8. Укажите получателей письма:

   - Установите курсор в поле **Кому** и введите электронные адреса получателей,

- Выберите получателей из адресной книги. Для этого установите курсор в поле **Кому** и в появившемся меню выберите действие **Показать все контакты**. Откроется окно со списком адресных книг с контактами. В списке отображаются только контакты с указанными email-адресами. Выберите один или несколько контактов. Для выбора контакта нажмите на его аватар.

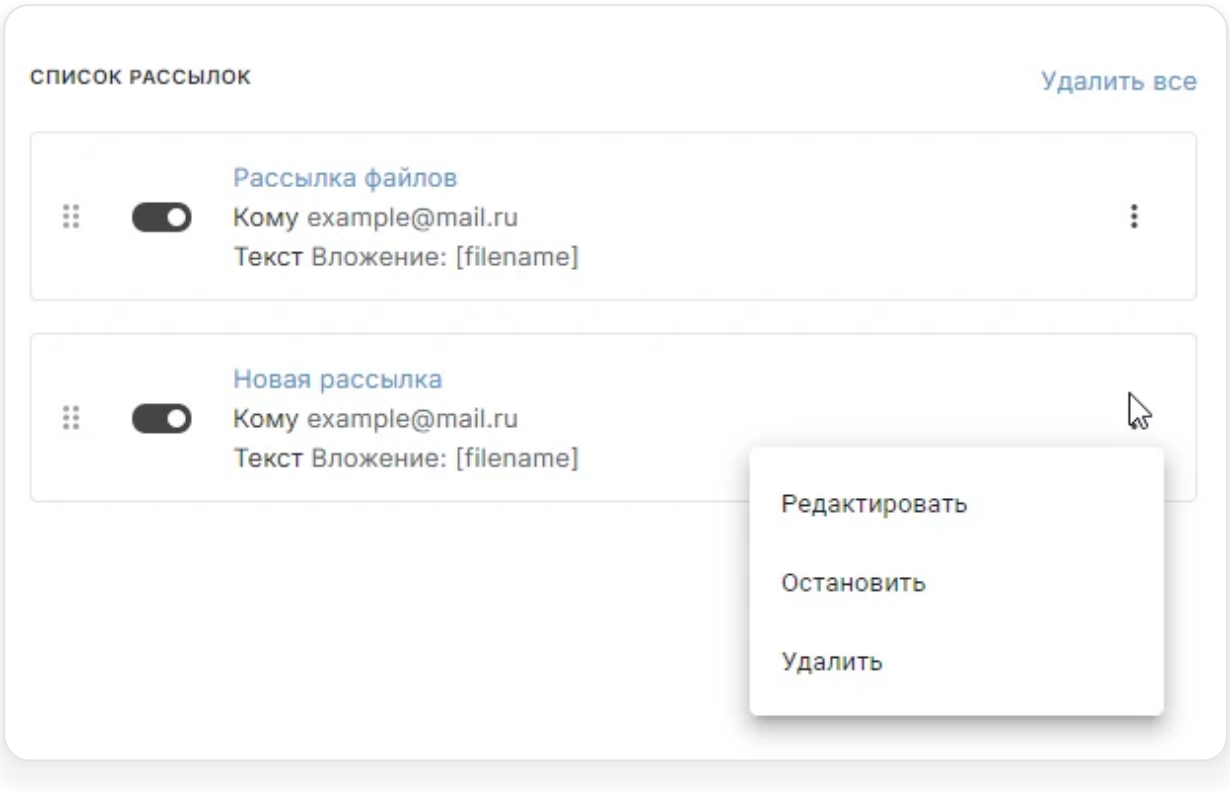


9. При необходимости активируйте запрос уведомлений о доставке и прочтении письма:
   - **Отследить доставку письма** - будет запрошено уведомление о доставке.
   - **Запросить подтверждение о прочтении письма** - будет запрошено уведомление о прочтении.
10. Дополнительно можно указать действия с файлами:
    - Отправленные файлы могут быть удалены с устройства либо перемещены в выбранную папку.
    - Файлы, которые не удалось отправить, можно удалить, оставить в исходной папке, либо переместить в выбранную папку.
11. Укажите настройки активности рассылки. Установите флаг **Запустить рассылку активной**, если нужно запустить рассылку сразу после сохранения;
12. Нажмите **Сохранить**.

Управление рассылками

1. Редактирование рассылки

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Рассылка файлов**.
3. Вызовите меню действий для рассылки, которую необходимо отредактировать.
4. Выберите **Редактировать**.



5. Откроется форма редактирования рассылки.
6. Внесите изменения.
7. Нажмите **Сохранить**.

2. Приостановка рассылки

Доступна временная приостановка рассылки без ее удаления.

Чтобы включить или отключить рассылку:

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Рассылка файлов**.
3. Отключите переключатель, размещенный на панели с рассылкой, либо нажмите **Остановить** в меню действий с рассылкой.

Изменения применяются автоматически без дополнительного подтверждения.

3. Удаление рассылки

Как удалить рассылку

Чтобы удалить одну рассылку файлов:

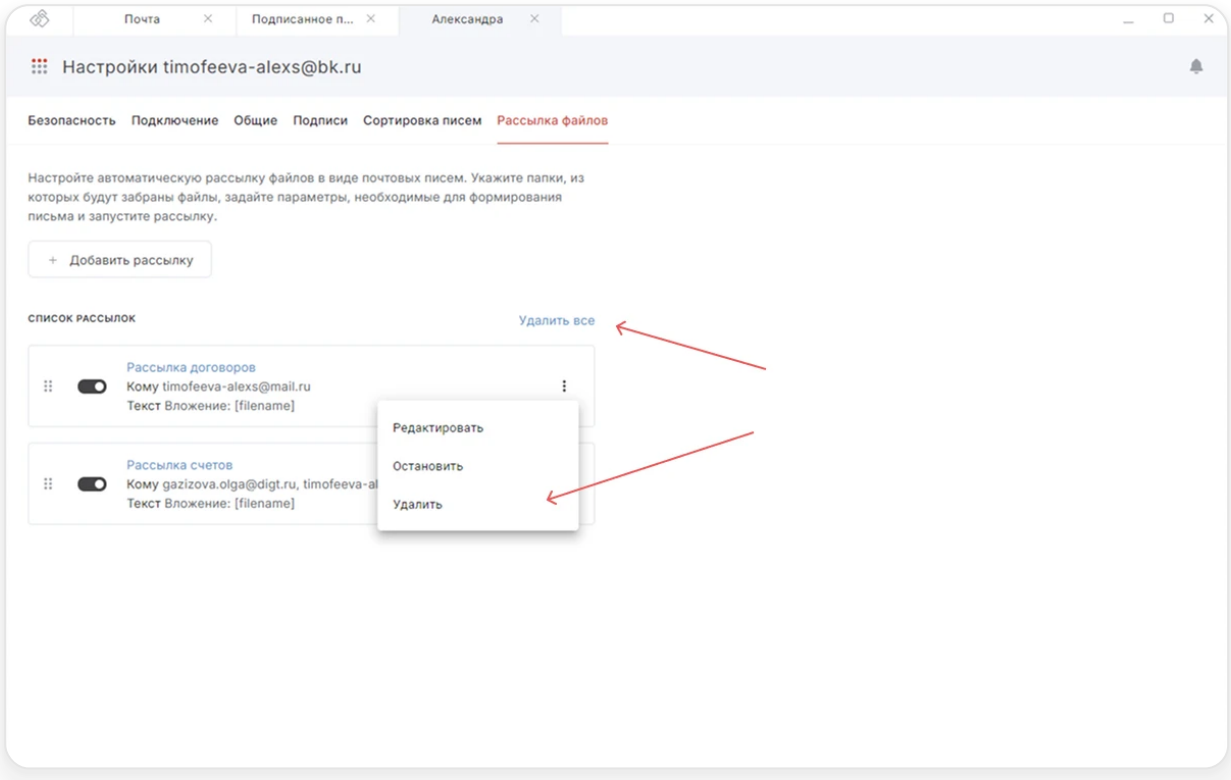
1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Рассылка файлов**.
3. Вызовите меню действий для рассылки, которую необходимо удалить.
4. Выберите **Удалить**.
5. Подтвердите действие в модальном окне.

Групповое удаление

> 🚨 **Внимание!** Это удалит **все** правила рассылки для этого аккаунта. Действие необратимо.

Чтобы удалить все рассылки файлов:

1. Откройте настройки почтового аккаунта. Как открыть настройки читайте в инструкции.
2. Перейдите на вкладку **Рассылка файлов**.
3. Нажмите кнопку **Удалить все**, размещенную над списком рассылок.
4. Подтвердите действие в модальном окне.



Инструкции по теме

- Проверка рабочего места
- Отправка подписанного и зашифрованного сообщения
- Действия с письмами
- Добавление почтового аккаунта
- Создание контакта

Открыть статью на сайте

Работа с расширениями .eml, .p7s, .p7m

- Формат EML (электронные письма)
- Формат P7M (зашифрованные письма)
- Формат P7S (подписанные письма)

Формат EML (электронные письма)

Основные сведения

EML — это файловый формат, разработанный компанией Microsoft для Outlook и Outlook Express.

Файлы этого формата:

- Сохраняют оригинальную структуру письма,
- Включают все заголовки и метаданные,
- Поддерживают HTML-форматирование,
- Могут содержать вложения.

Открытие письма в формате .eml

Если у вас на компьютере сохранен файл с письмом `.eml`, вы можете открыть его с помощью КриптоАРМ одним из способов:

1. **Способ 1** (через контекстное меню):
    - Вызовите контекстное меню для письма в формате `.eml` в файловом менеджере или на рабочем столе.
    - Выберите пункт **Открыть с помощью** и далее выберите программу КриптоАРМ.
2. **Способ 2** (двойной клик):
    - Убедитесь, что EML-файлы ассоциированы с КриптоАРМ,
    - Дважды щелкните по файлу,

После открытия письмо отображается в новой вкладке с сохранением всех оригинальных элементов.

> 💡 **Совет**: Вы можете импортировать письмо `.eml` в любой из подключенных аккаунтов.

Формат P7M (зашифрованные письма)

Основные сведения

Во входящих письмах могут отображаться файлы с расширением `.p7m`, это говорит о том, что данное письмо зашифровано и не удалось расшифровать контент письма. В приложении КриптоАРМ такие письма определяются как зашифрованные и отображается соответствующая иконка на письмах.

Расшифрование письма в формате.p7m

Если у вас на компьютере сохранен файл с зашифрованным письмом `.p7m`, вы можете расшифровать его с помощью КриптоАРМ одним из способов:

1. **Способ 1**:
    - Запустите приложение КриптоАРМ.
    - Перейдите в раздел **Документы**.
    - Откройте мастер **Проверка и расшифрование**.
    - Добавьте в мастер файл с расширением .p7m.
    - Выполните расшифрование.
2. **Способ 2** (двойной клик):
    - Убедитесь, что p7m-файлы ассоциированы с КриптоАРМ,
    - Дважды щелкните по файлу,
    - Откроется мастер **Проверка и расшифрование**,
    - Выполните расшифрование.

В результате зашифрованная часть письма будет расшифрована, и вы получите файл с расширением `.eml`, который можно будет просмотреть как обычное письмо в отдельной вкладке.

Формат P7S (подписанные письма)

Основные сведения

Расширение файла .p7s означает, что данный файл содержит электронную подпись. В случае с письмами, внутри подписанного письма могут находиться файлы в виде `smime.p7s`. В приложении КриптоАРМ такие письма определяются как подписанные и отображается соответствующая иконка на письмах. В сторонних приложениях проверить подпись таких писем не всегда возможно.

Проверка подписи письма с вложением smime.p7s

1. Скачайте письмо в формате `.eml` через веб-интерфейс почтового сервиса или через сторонний почтовый клиент.

2. Откройте письмо в формате `.eml` в приложении КриптоАРМ.
3. В окне просмотра письма будет отображаться иконка .

   В зависимости от статуса подписи письма иконка будет иметь цвет:

   - зеленый цвет, если подпись письма действительная,
   - красный цвет, если подпись недействительная,
   - серый цвет, если статус подписи неизвестен

4. Нажмите на иконку .
5. Откроется окно со статусом подписи, датой подписания и проверки.
6. Для просмотра детальной информации о подписи нажмите **Подробнее**.

Инструкции по теме

- Сохранение письма на компьютере
- Проверка рабочего места
- Отправка подписанного и зашифрованного сообщения
- Добавление почтового аккаунта

Открыть статью на сайте

Управление профилями

- О профилях подписи
- Создание профиля
- Редактирование настроек профиля
- Переключение между профилями
- Экспорт профиля
- Импорт профиля подписи
- Удаление профилей

О профилях подписи

Профили подписи — это готовые наборы настроек, которые можно применять для выполнения подписи, архивирования и шифрования в мастерах **Подпись и шифрование** и **Подпись и защита PDF**.

Советы по работе:

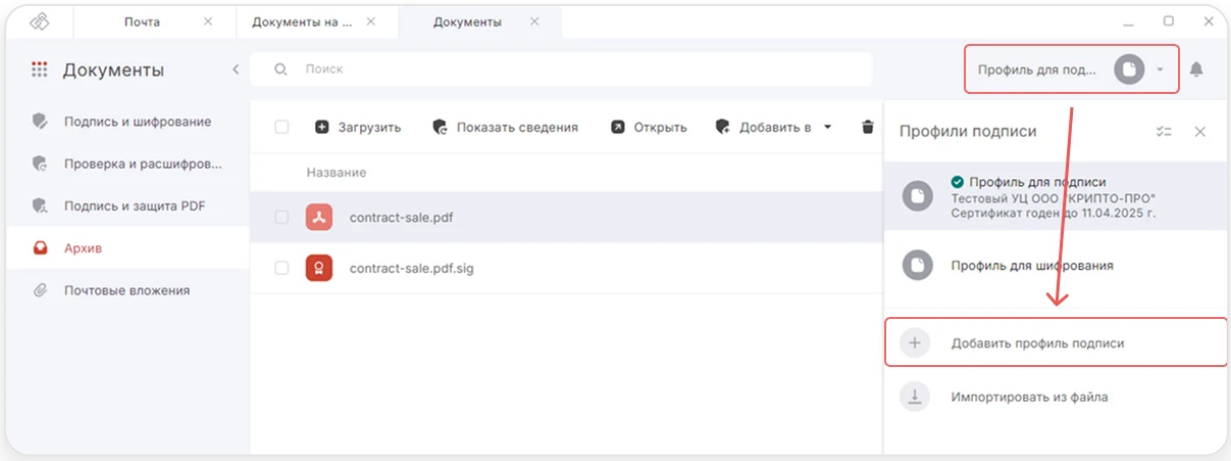
- Создавайте отдельные профили для разных задач и типов операций,
- Проверяйте актуальность сертификатов в профилях,
- Используйте экспорт/импорт для синхронизации между устройствами,
- Для важных операций проверяйте актуальность параметров профиля.

Создание профиля

> 💡 **Совет**: Начните с создания базовых профилей для самых частых операций, затем постепенно добавляйте специализированные настройки по мере необходимости.

1. Стандартный способ

1. Перейдите в раздел **Документы**.
2. Откройте окно со списком профилей. Для этого нажмите на название активного профиля в верхнем правом углу окна.
3. Выберите **Добавить профиль подписи**.



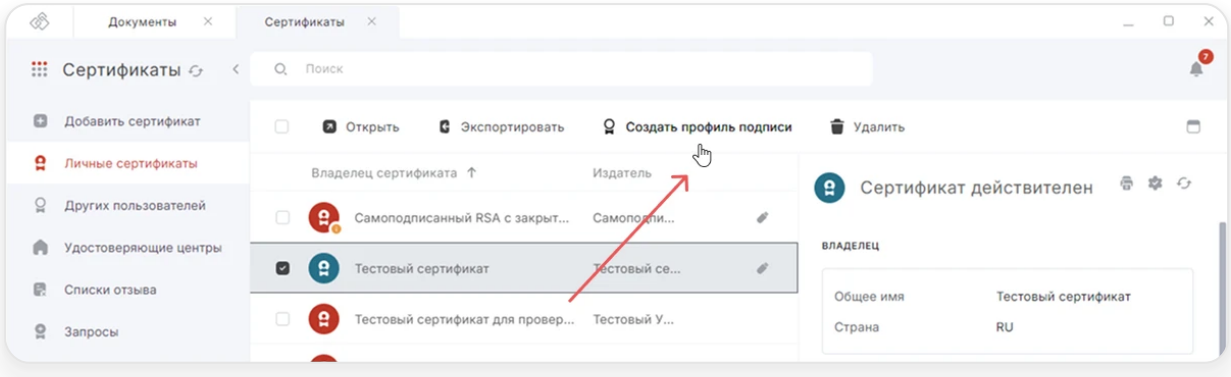
4. Откроется окно **Новый профиль**.
5. Укажите настройки.

> 🔍 Подробнее про настройки в инструкции Описание настроек профиля.

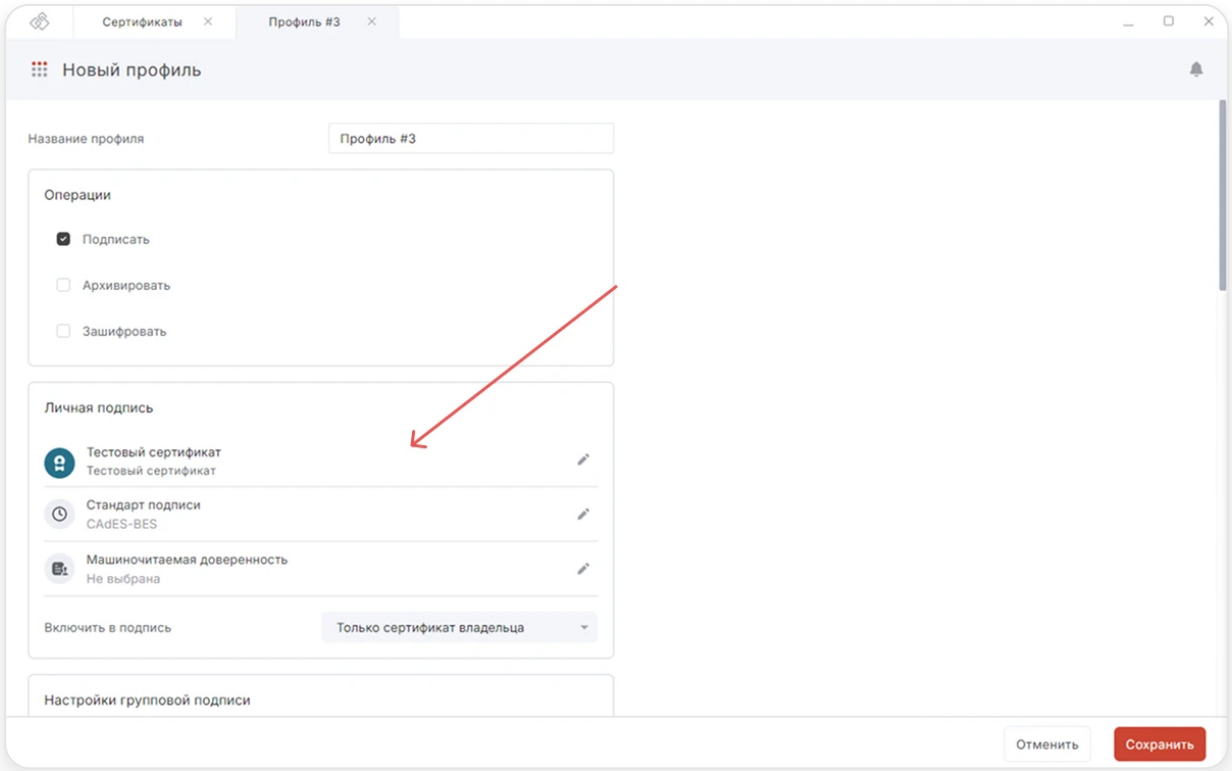
6. Нажмите **Сохранить**.

2. Создание из сертификата

1. Перейдите в раздел **Сертификаты** → хранилище **Личные сертификаты**.
2. Выделите личный сертификат, с помощью которого необходимо создать профиль подписи.
3. На панели действий нажмите на кнопку **Создать профиль подписи**.



4. Откроется окно **Новый профиль**. Личный сертификат будет автоматически привязан в блоке **Личная подпись**.



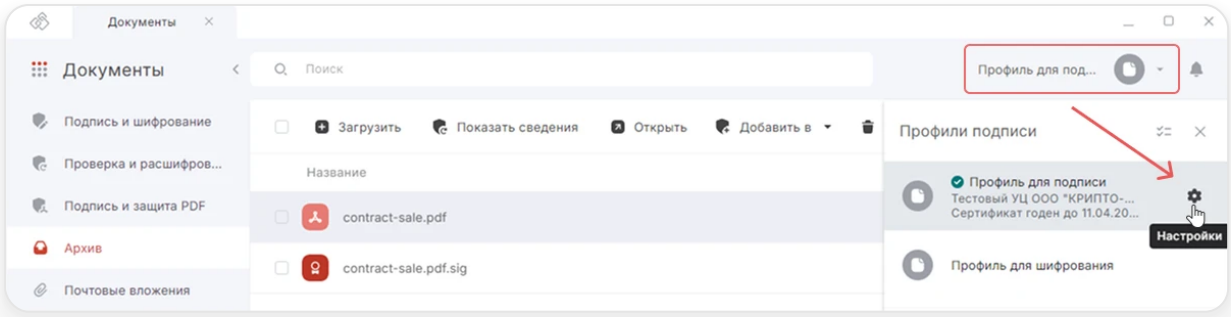
5. Укажите остальные настройки.

> 🔍 Подробнее про настройки в инструкции Описание настроек профиля.

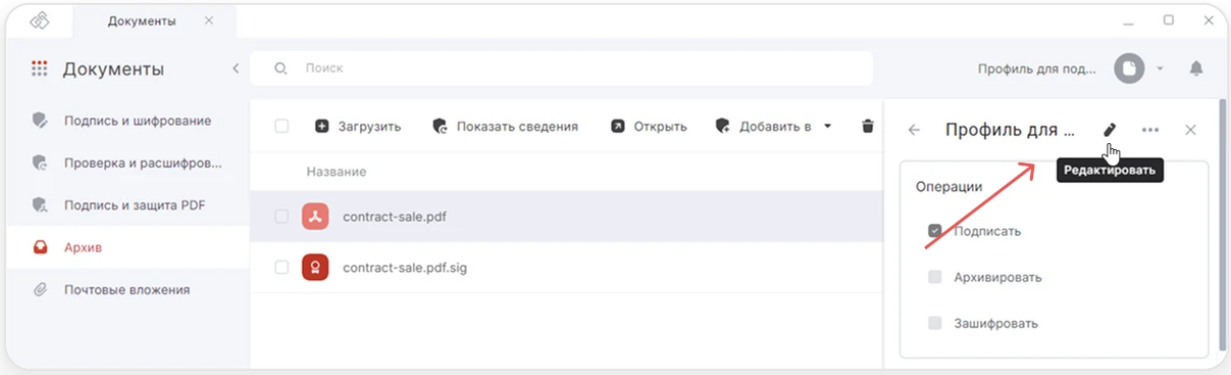
6. Нажмите **Сохранить**.

Редактирование настроек профиля

1. Перейдите в раздел **Документы**.
2. Откройте окно со списком профилей. Для этого нажмите на название активного профиля в верхнем правом углу окна.
3. Наведите на панель с профилем, настройки которого необходимо отредактировать.
4. Нажмите на кнопку **Настройки** .



5. Откроется окно с предпросмотром настроек.
6. Нажмите на кнопку **Редактировать** .



7. Откроется форма для редактирования настроек профиля.
8. Внесите изменения в настройки.

> 🔍 Подробнее про настройки в инструкции Описание настроек профиля подписи.

9. Нажмите кнопку **Сохранить**.

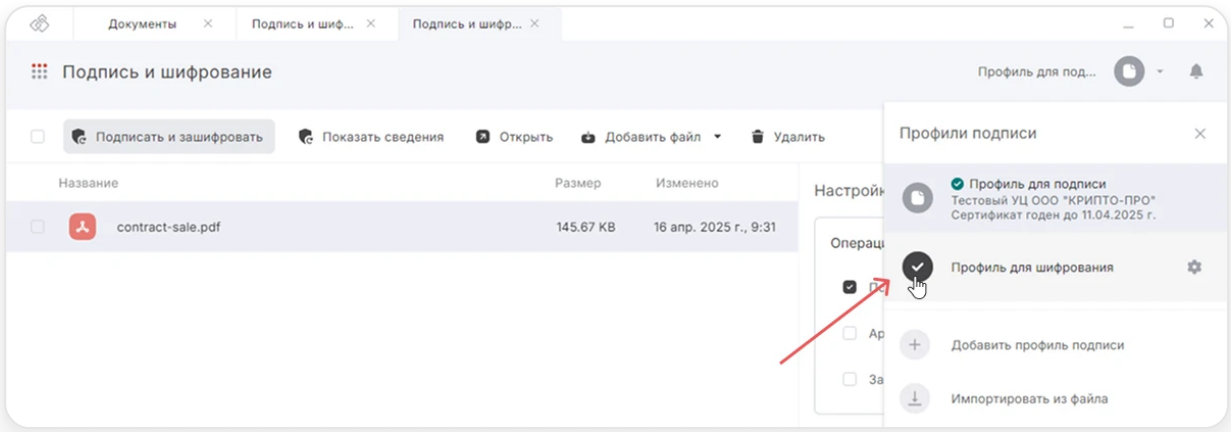
Переключение между профилями

> 💡 По умолчанию в мастерах применяются настройки из активного профиля подписи.

Вы можете переключаться между профилями подписи для выполнения операций с заранее настроенными параметрами в профилях.

Чтобы переключить профиль:

1. Перейдите в раздел **Документы**.
2. Откройте мастер **Подпись и шифрование** или **Подпись и защита PDF**.
3. Вызовите окно со списком профилей. Для этого нажмите на название активного профиля в верхнем правом углу окна.
4. Нажмите на иконку профиля, который хотите сделать активным.

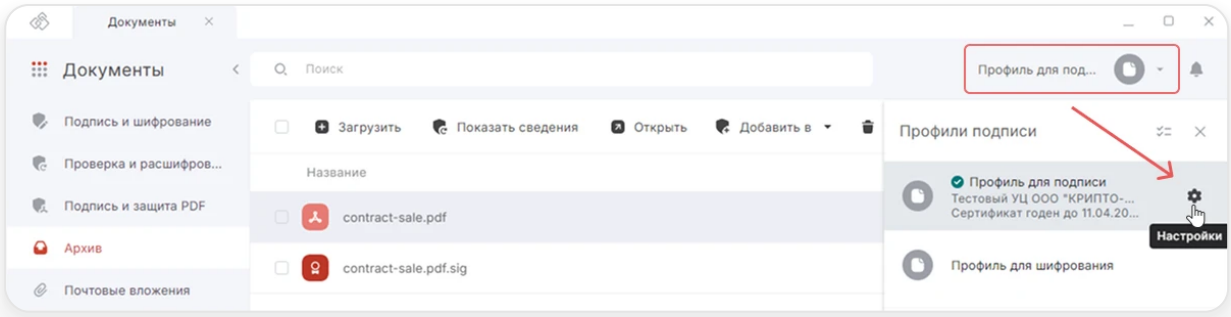


Экспорт профиля

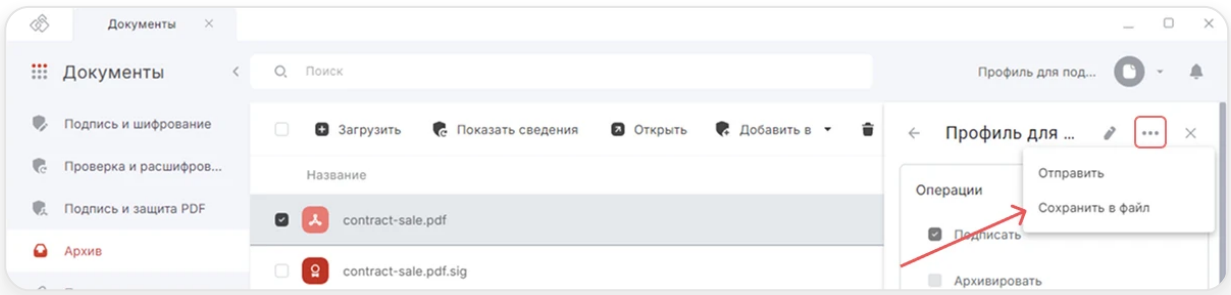
> ⚠️ **Что НЕ экспортируется:** 1. **Закрытые ключи** сертификатов — никогда не покидают вашу систему. 2. **Пароли/пин-коды** к контейнерам или токенам. 3. **Файлы на диске** (например, МЧД, указанные в настройках) — экспортируется только путь, который на другом компьютере будет нерабочим.

1. Экспорт профиля в файл

1. Перейдите в раздел **Документы**.
2. Откройте окно со списком профилей. Для этого нажмите на название активного профиля в верхнем правом углу окна.
3. Наведите на панель с профилем и нажмите на появившуюся кнопку **Настройки** .



4. Откроется окно с предпросмотром настроек.
5. Вызовите меню действий с профилем по кнопке **Еще** ••• .
6. Выберите **Сохранить в файл**.

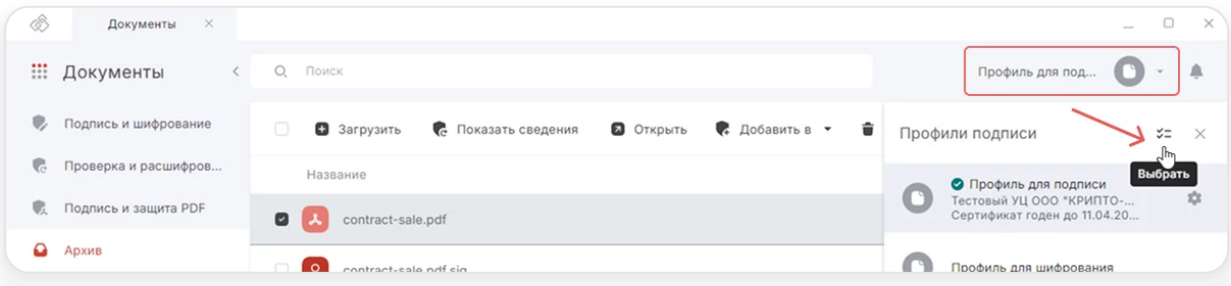


7. Укажите путь для сохранения файла с профилем.

В результате по указанному пути будет сохранён файл с расширением .pcarm.

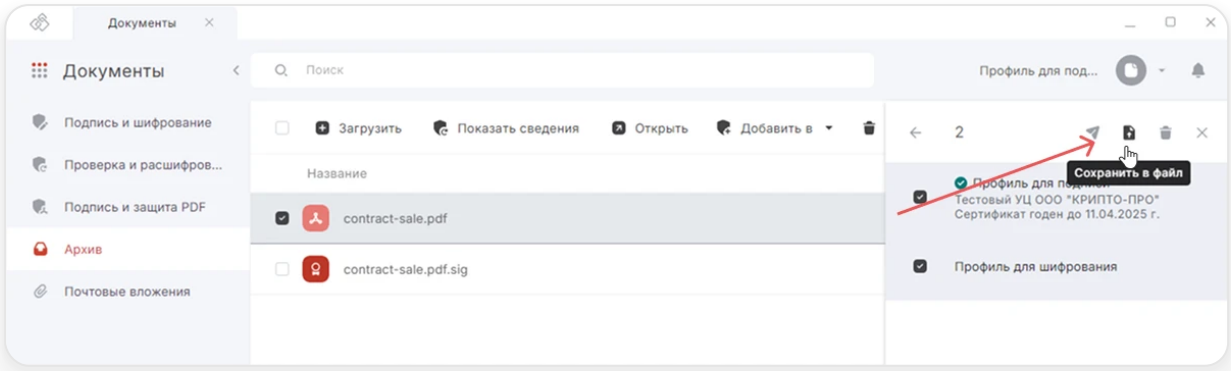
2. Групповой экспорт в файл

1. Перейдите в раздел **Документы**.
2. Откройте окно со списком профилей. Для этого нажмите на название активного профиля в верхнем правом углу окна.
3. Нажмите кнопку **Выбрать** ☑ .



4. Отметьте флагами профили, которые вы хотите экспортировать.

5. Нажмите кнопку **Сохранить в файл**.



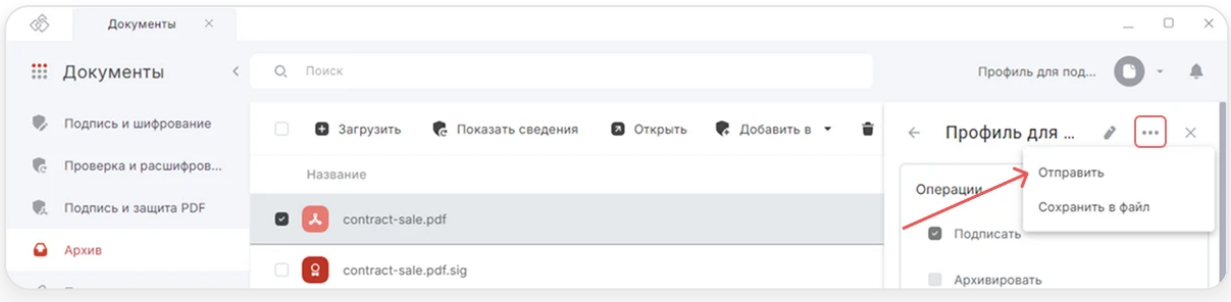
6. Укажите путь для сохранения файла профиля.

Профили будут сохранены в файл с расширением .pcarm

3. Отправка профиля по почте

> ⚠️ **Примечание**: Для отправки профилей подписи по почте в приложении должен быть подключен почтовый аккаунт.

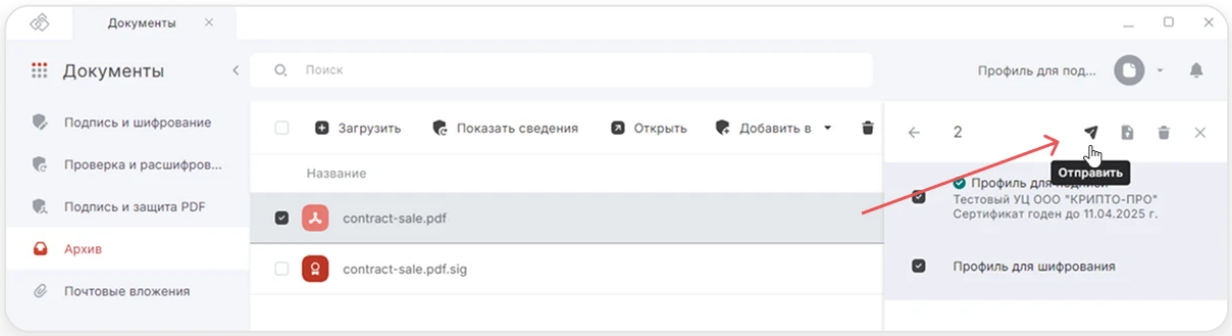
1. Перейдите в раздел **Документы**.
2. Откройте окно со списком профилей. Для этого нажмите на название активного профиля в верхнем правом углу окна.
3. Наведите на панель с профилем и нажмите на появившуюся кнопку **Настройки** .
4. Откроется окно с предпросмотром настроек.
5. Вызовите меню действий с профилем по кнопке **Еще** .
6. Выберите **Отправить**.



7. Откроется вкладка **Новое письмо**, в котором во вложении будет прикреплен профиль подписи с расширением .pcarm.
8. Заполните обязательные поля и отправьте письмо.

4. Групповая отправка по почте

1. Перейдите в раздел **Документы**.
2. Откройте окно со списком профилей. Для этого нажмите на название активного профиля в верхнем правом углу окна.
3. Нажмите кнопку **Выбрать** .
4. Отметьте флагами профили, которые вы хотите отправить по почте.
5. Нажмите кнопку **Отправить** .



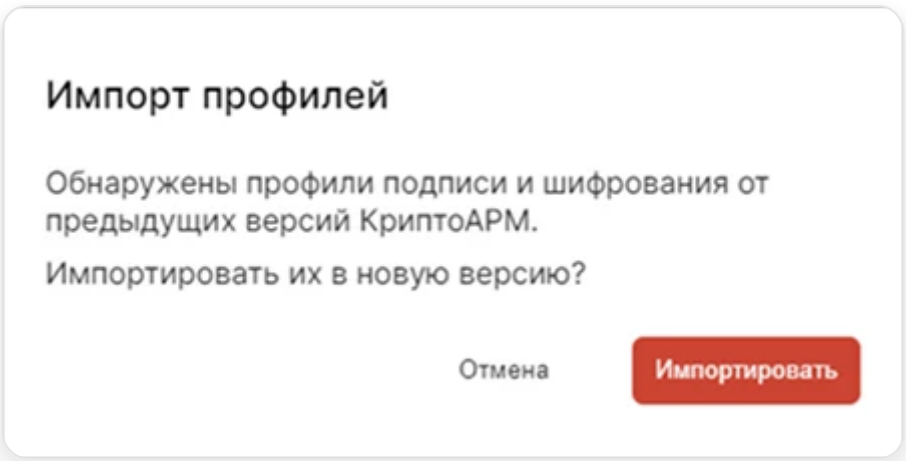
6. Откроется вкладка **Новое письмо**, в котором во вложении будет прикреплен профиль подписи с расширением .pcarm.

Импорт профиля подписи

1. Автоматический импорт из других версий КриптоАРМ

Автоматический импорт доступен при первом запуске приложения.

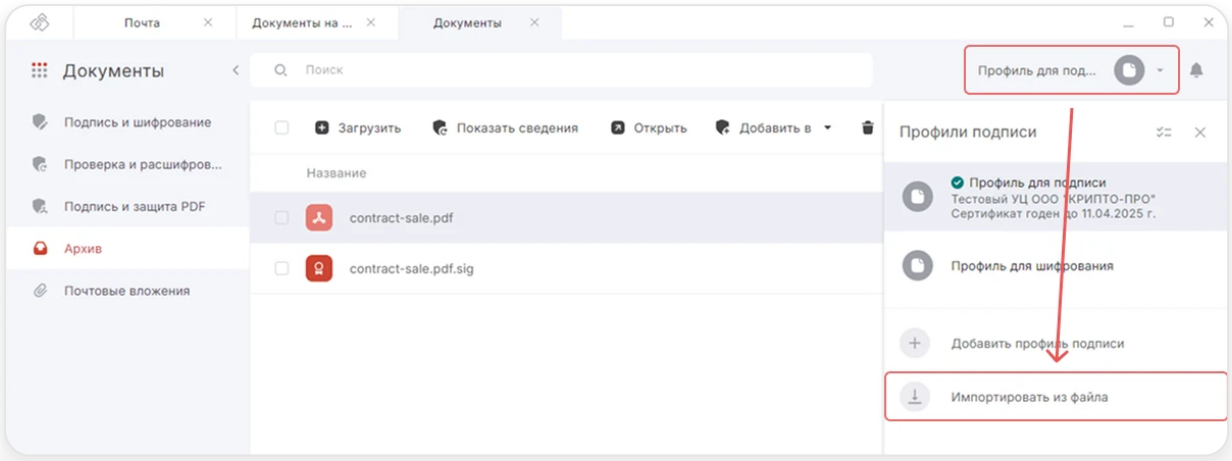
Если в системе будут обнаружены профили подписи из предыдущих версий КриптоАРМ, появится диалоговое окно с предложением импортировать эти профили.



2. Импорт профиля из файла

Способ 1 (из приложения):

1. Перейдите в раздел **Документы**.
2. Откройте окно со списком профилей. Для этого нажмите на название активного профиля в верхнем правом углу окна.
3. Нажмите кнопку **Импортировать из файла**.



4. В открывшемся окне файлового менеджера выберите файл профиля подписи в формате .pcarm, .json или .xml.
5. При успешном импорте профиль сохранится в приложении и будет отображаться в списке профилей.

Способ 2 (из файловой системы):

1. Дважды кликните по файлу, либо правой кнопкой мыши вызовите контекстное меню для файла и выберите пункт **Открыть с помощью КриптоАРМ**.
2. После выполнения данных действий запустится приложение КриптоАРМ (если не было запущено) и профиль автоматически импортируется в приложение.

3. Импорт профиля из письма

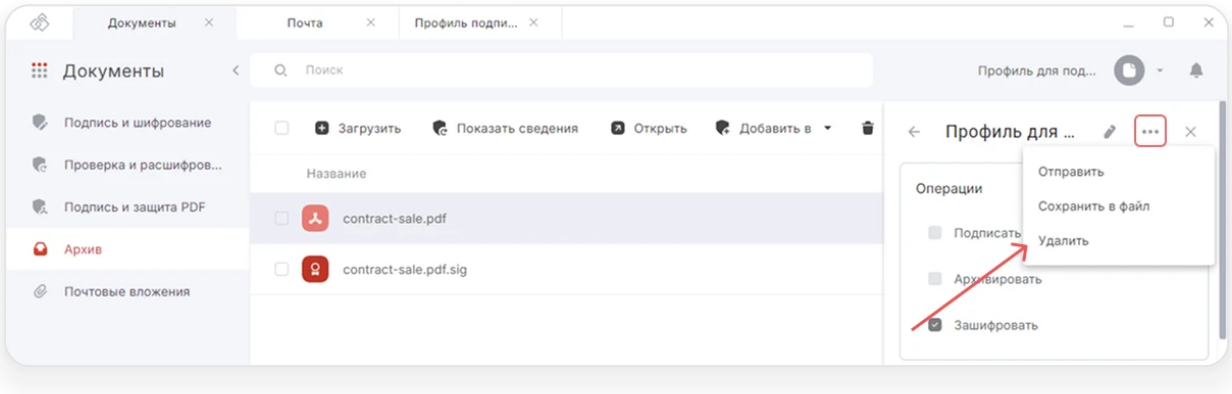
1. Перейдите в раздел **Почта**.
2. Откройте письмо, которое содержит во вложении профиль подписи в формате .pcarm.
3. Выполните действие одним из способов:
   - Кликните по названию файла в формате .pcarm,
   - Вызовите меню действий с вложением по кнопке **Еще** и выберите действие **Импортировать профиль**.

Удаление профилей

> ⚠️ **Примечание**: Активный профиль удалить невозможно. Сначала переключитесь на другой профиль.

1. Как удалить профиль подписи

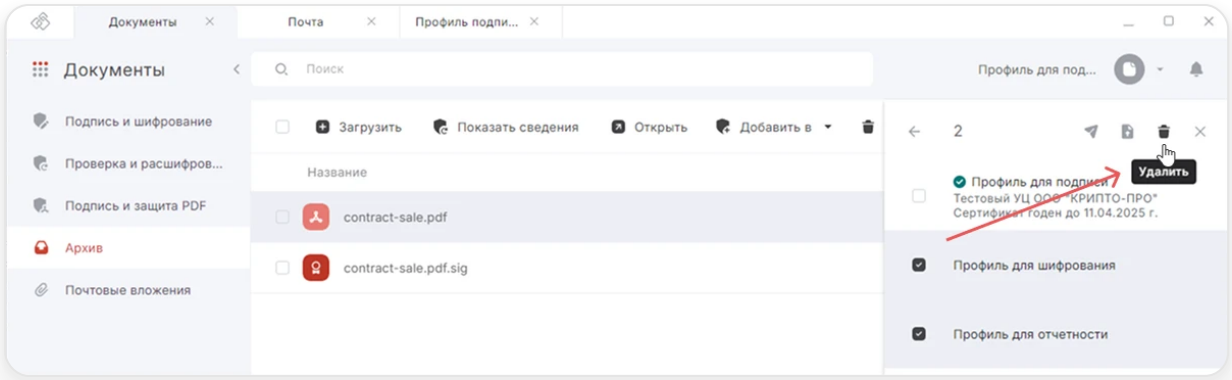
1. Перейдите в раздел **Документы**.
2. Откройте окно со списком профилей. Для этого нажмите на название активного профиля в верхнем правом углу окна.
3. Наведите курсор на тот профиль, который хотите удалить.
4. Нажмите на кнопку **Настройки** .
5. Откроется окно с предпросмотром настроек.
6. Вызовите меню действий с профилем по кнопке **Еще** .
7. Нажмите **Удалить**.



8. Подтвердите действие в модальном окне.

2. Групповое удаление

1. Перейдите в раздел **Документы** или в мастер **Подпись и шифрование**.
2. Откройте окно со списком профилей. Для этого нажмите на название активного профиля в верхнем правом углу окна.
3. В окне со списком профилей нажмите на кнопку **Выбрать** .
4. Отметьте флагами профили, которые вы хотите удалить.
5. Нажмите кнопку **Удалить** .



6. Подтвердите действие в модальном окне.

Инструкции по теме

- Подпись документов со стандартом CAdES
- Подпись документов со стандартом PAdES
- Добавление соподписи

Открыть статью на сайте

Описание настроек профиля

- Операции
- Личная подпись
- Настройки групповой подписи
- Настройки подписи CAdES
- Настройки подписи PAdES
- Настройки защиты PDF-документа
- Настройки конвертации в PDF/A
- Настройки печатной формы для PDF-документов
- Сертификаты шифрования
- Настройки шифрования
- Сохранение результатов

Операции

Название настройки	Тип	Значение по умолчанию	Описание	Дополнительные параметры
Выбор операций	Множественный выбор (чекбоксы)	`Подпись`	Определяет набор действий, применяемых к документу	`Подпись`, `Архивирование`, `Шифрование`

Личная подпись

> 🔐 Стандарты `CAdES-T`, `CAdES-A` и `CAdES-X Long Type 1` доступны для сертификатов, установленных в хранилище криптопровайдера КриптоПро CSP.
>
> 🔐 Стандарты `CAdES-T`, `CAdES-A` и `CAdES-X Long Type 1` доступны только при наличии установленных модулей КриптоПро TSP Client и КриптоПро OCSP Client и лицензий на них.

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
Личный сертификат	Поле для выбора сертификата	-	Личный сертификат, который будет	Сертификат их хранилища **Личные**

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
			использоваться для подписи документов.	
Стандарт подписи	Выпадающий список	`CAdES-BES`	Выбор стандарта электронной подписи.	- `CAdES-BES` (классическая подпись), - `CAdES-T` (со штампом времени), - `CAdES-A` (с архивным штампом), - `CAdES-X Long Type 1` (усовершенствованная)
Машиночитаемая доверенность	Поле для выбора файла	-	Путь к файлу доверенности и её подписи. Доверенность будет включена в пакет документов.	Файлы с расширением `.xml` и `.sig`.
Включить в подпись	Выпадающий список	`Только сертификат владельца`	Определяет, какие сертификаты добавляются в атрибуты подписи.	- `Только сертификат владельца`, - `Цепочка без корневого сертификата`, - `Все сертификаты цепочки`

Настройки для стандартов со штампами

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
Служба штампов времени (TSP)	Текстовое поле	-	Адрес службы штампов времени. Адрес службы можно узнать у поставщика услуги. Услуги службы штампов времени могут предоставлять удостоверяющие центры.	Формат адреса: `<https>://<сервер>[:порт][/путь]`

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
Служба онлайн статусов (OCSP)	Текстовое поле	-	Адрес службы онлайн-статусов. Данное поле **необязательно** для заполнения, чаще всего адрес прописан в сертификате подписи.	Формат адреса: `<https>://<сервер>[:порт][/путь]`

Настройки прокси сервера

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
Адрес прокси сервера	Текстовое поле	-	IP-адрес или доменное имя прокси-сервера	IPv4/IPv6 адрес или валидное доменное имя
Порт	Числовое поле	-	Номер порта для подключения к прокси	Стандартные порты: 80 (HTTP), 3128 (Squid), 8080 (альтернативный HTTP)
Логин	Поле для ввода	-	Имя пользователя для доступа к прокси	Любая строка до 64 символов
Пароль	Поле для ввода	-	Пароль для доступа к прокси	Любая строка до 128 символов

Настройки групповой подписи

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
Создать отдельный пакет (архив) для каждого документа	Переключатель (On/Off)	`Off`	Если включено, система создаст отдельный ZIP-архив для каждого подписываемого файла. В этот архив будут помещены все файлы,	`On` / `Off`

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
			созданные в результате подписи.	
Использовать PAdES для PDF	Переключатель (On/Off)	`Off`	Если включено, PDF-документы будут подписаны встроенной подписью по стандарту PAdES вместо CAdES.	`On` / `Off`

Настройки подписи CAdES

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
Кодировка подписи	Выпадающий список	`DER`	Определяет способ кодирования данных подписи.	`DER` (стандартная бинарная кодировка), `BASE-64` (текстовая кодировка)
Отключить служебные заголовки	Переключатель (On/Off)	`Off`	Доступен для кодировки `BASE-64`. Убирает заголовки `-----BEGIN CERTIFICATE-----` и `-----END CERTIFICATE-----`.	`On` / `Off`
Вид подписи	Выпадающий список	`Присоединенная`	Выбор формата хранения подписи относительно документа.	- `Присоединенная` (подпись и документ в одном файле), - `Отсоединенная` (подпись хранится отдельно)
Формат файла подписи	Выпадающий список	`.sig`	Расширение файла, в который сохраняется подпись.	`.sig`, `.p7s`, `.sgn`, `.sign`, `.bin`

Настройки подписи PAdES

Настройка внешнего вида штампа подписи

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
Вид штампа	Выпадающий список	`Штамп`	Определяет внешний вид штампа	- `Штамп`, - `Штамп с реквизитами слева`, - `Штамп с реквизитами справа`, - `Штамп с реквизитами с обеих сторон`
Реквизиты	Выпадающий список	`По ГОСТу`	Определяет набор отображаемых реквизитов в штампе	- `По ГОСТу` (стандартный набор в соответствии с ГОСТ Р 7.0.97-2016), - `Произвольно` (ручная настройка реквизитов)
Добавить фон на область	Переключатель (On/Off)	`On`	Настройка фона штампа. Если включено, в штамп будет добавлен фон #ffffff (hex)	`On` / `Off`
Добавить границу	Переключатель (On/Off)	`On`	Настройка границы штампа. Если включено, в штамп будет добавлена граница.	`On` / `Off`
Настроить цвет границы и текста	Поле для ввода значения в hex-формате/Выбор цвета в палитре	`#000`	Настройка границы и текста в штампе.	Значение в hex-формате
Логотип	Поле загрузки файла	-	Позволяет добавить логотип в штамп	Файлы изображений (`.webp`, `.jpg`, `.svg`). Максимальный размер - 10 МБ.

Настройка положения штампа подписи

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
Видимость подписи	Выпадающий список	Видимая подпись	Определяет визуальное отображение подписи на документе	- Видимая подпись (отображается как штамп), - Невидимая подпись (подпись существует, но не видна)
Размер штампа	Поля ввода значения в миллиметрах	Ширина 102,30 мм, Высота 39,16 мм	Позволяет задать точные размеры штампа подписи	Ширина от 1 до 207.9 мм, Высота от 1 до 294.69 мм (Используется значение для формата A4)
Ориентация	Выпадающий список	0°	Настройки ориентации штампа	0°, 90°, 180°, 270°
Страница расположения	Выпадающий список	Последняя	Страница расположения штампа	- Последняя, - Указать страницу (выбор страницы)
Добавить копию изображения штампа на все страницы	Переключатель (On/Off)	Off	Если включено, на все страницы документа добавляется копия изображения штампа	On / Off
Координаты расположения штампа	Поля ввода значения в миллиметрах	Y 20 мм, X 66,60 мм	-	- Y от 1 до 256.53 мм, - X от 1 до 106.60 мм (Для размера штампа по умолчанию)

Настройка внешнего вида произвольной области

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
Вид	Выпадающий список	Оставить пустым		- Оставить пустым (следующий подписант может

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
			Определяет внешний вид области, которая будет добавлена в документ	добавить комментарий/ статус), - `Изображение` (загрузка готовой графической отметки), - `Текст` (ввод произвольного текста)

Настройки защиты PDF-документа

Название настройки	Тип	Значение по умолчанию	Описание	Дополнительные параметры
Сертифицировать	Переключатель (On/Off)	`Off`	Включает режим сертификации PDF с защитой от изменений. Разрешает только: заполнение размеченных областей подписантами и произвольных полей.	`On` / `Off`
Конвертировать в PDF/A	Переключатель (On/Off)	`Off`	Преобразует документ в архивный формат PDF/A с удалением потенциально опасных элементов: скриптов, динамических форм и нестандартных шрифтов.	`On` / `Off`

Настройки конвертации в PDF/A

> ⚠️ **Примечание**: Если вы конвертируете документ с форматом PDF/A-3b в PDF/A-2b, все вложенные файлы внутри документа будут удалены, потому что формат PDF/A-2b не поддерживает встроенные объекты.

Название настройки	Тип	Значение по умолчанию	Описание	Дополнительные параметры
Формат PDF/A	Выпадающий список	`PDF/A-2b`	Настройка формата конвертации	- `PDF/A-2b` — стандарт для архивирования PDF-документов, обеспечивает визуальную совместимость. Документ хранится как PDF, без возможности включать другие файлы. - `PDF/A-3b` — расширение формата PDF/A-2b, позволяет встраивать любые файлы (например XML, CSV) внутрь PDF для архивирования вместе с исходными данными.
Если при конвертации возникнут ошибки	Радио-кнопки	`Преобразовать страницы с ошибками в изображения`	Настройка поведения при возникновении ошибок в ходе конвертации	- `Преобразовать страницы с ошибками в изображения`, - `Преобразовать все страницы в изображения`
Разрешение изображений	Выпадающий список	`150 ppi`	Настройка разрешения изображений для преобразованных страниц	- `70 ppi`, - `100 ppi`, - `150 ppi`, - `200 ppi`, - `300 ppi`,
Безопасный режим	Переключатель (On/Off)	`Off`	При включении активируется медленный режим	`On` / `Off`

Название настройки	Тип	Значение по умолчанию	Описание	Дополнительные параметры
			работы. В этом режиме страницы обрабатываются по очереди друг за другом.	

Настройки печатной формы для PDF-документов

Название настройки	Тип	Значение по умолчанию	Описание	Дополнительные параметры
Создать печатную форму для PDF-документов со штампом подписи	Переключатель (On/Off)	`Off`	Для PDF-документов создается копия исходного документа, в который помещается изображение штампа подписи. Печатная форма не содержит подпись.	`On` / `Off`

Настройки внешнего вида штампа в печатной форме

Настройки аналогичны Настройкам подписи PAdES.

Настройки положения штампа в печатной форме

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
Размер штампа	Поля ввода значения в миллиметрах	Ширина `102,30 мм`, Высота `39,16 мм`	Позволяет задать точные размеры штампа подписи	Ширина от `1 до 207.9 мм`, Высота от `1 до 294.69 мм` (Используется значение для формата A4)
Ориентация	Выпадающий список	`0°`	Настройки ориентации штампа	`0°`, `90°`, `180°`, `270°`
		`Все`		

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
Страница расположения	Выпадающий список		Страница расположения штампа	`Все`, `Некоторые (выбор страницы)`, `Последняя`
Координаты расположения штампа	Поля ввода значения в миллиметрах	Y `20 мм`, X `66,60 мм`	-	Y от `1 до 256.53 мм`, X от `1 до 106.60 мм` (Для размера штампа по умолчанию)

Сертификаты шифрования

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
Сертификаты шифрования	Поле для выбора сертификатов	-	Сертификаты, которые будут использоваться при шифровании	- Сертификаты из хранилищ **Личные** и **Других пользователей**, - Контакты с сертификатами

Настройки шифрования

> 🔐 ГОСТ-алгоритмы шифрования доступны при установленном криптопровайдере КриптоПро CSP.

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
Алгоритм шифрования	Выпадающий список	`ГОСТ Р 34.12-2015 Магма`	Определяет алгоритм, используемый для шифрования данных	`ГОСТ 28147-89` (устаревший), `ГОСТ Р 34.12-2015 Магма` (актуальный), `ГОСТ Р 34.12-2015 Кузнечик` (256-битный), `AES 256 CBC`, `DES3-CBC`

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
Кодировка файлов	Выпадающий список	`DER`	Задает способ представления зашифрованных данных	`DER`, `BASE-64`
Формат файла	Выпадающий список	`.enc`	Определяет расширение для зашифрованных файлов	`.enc` (стандартное), `.p7m`, `.p7e`, `.pem`
Удалить исходные файлы	Переключатель (On/Off)	`Off`	Удаляет оригинальные файлы после успешного шифрования	`On` / `Off`

Сохранение результатов

Название настройки	Тип	Значение по умолчанию	Описание	Дополнительные параметры
Сохранение результатов	Радио-кнопки	`Папка с исходным документом`	Определяет место сохранения результатов операции	- `Папка с исходным документом` (сохраняет рядом с оригиналом), - `Сохранить в папку...` (ручной выбор пути)
Создать копию в папке «Архив»	Переключатель (On/Off)	`Off`	Дополнительное сохранение результатов в специальную папку приложения	`On` / `Off`

Открыть статью на сайте

Подпись со стандартом CAdES

- О подписи CAdES
- Подпись документов
- Подписание сертификатом DSS
- Возможные ошибки

О подписи CAdES

В КриптоАРМ можно создать электронную подпись файлов со стандартами:

- **CAdES-BES** - базовая подпись без меток времени,
- **CAdES-T** - подпись со штампом времени (TSP) для фиксации момента подписания,
- **CAdES-A** - для создания подписи с архивными штампами времени,
- **CAdES-X Long Type 1** - для создания усовершенствованной подписи. Расширяет стандарт CAdES-A: сохраняет полные доказательства валидации и цепочки сертификатов.

Подпись может быть добавлена в файл как присоединенная или отсоединенная.

При присоединенной подписи документ и подпись хранятся в одном файле. Для подписанного документа создается новый файл расширением (например, `.p7s` или `.sig`). Что делает невозможным открытие файла без снятия подписи с помощью специализированного приложения. Основное преимущества такого варианта — удобство хранения и передачи.

Отсоединенная подпись сохраняется в отдельном файле (обычно с расширением `.p7s` или `.sig`). Исходный документ остается неизменным и доступным для просмотра.

> 💡 **Совет**: В мастере «Подпись и шифрование» вы можете выполнить подпись PDF-файлов со стандартом PAdES. Подробнее читайте в инструкции Подпись PDF-документов.

Подпись документов

> 💡 **С чего начать**: Чтобы оценить, готово ли ваше рабочее место для работы с электронной подписью, воспользуйтесь Проверкой рабочего места.

Шаг 1. Запуск мастера

1. Перейдите в раздел **Документы**.

2. Нажмите **Подпись и шифрование** в боковом меню раздела **Документы**.
3. Откроется новая вкладка с мастером.

> 💡 **Совет**: Открыть мастер можно с помощью действия **Добавить в** → **Подпись и шифрование** для файла в папке «Архив», результатах операции или в разделе «Почта».

Шаг 2. Добавление документов

Добавьте документы в мастер одним из способов:

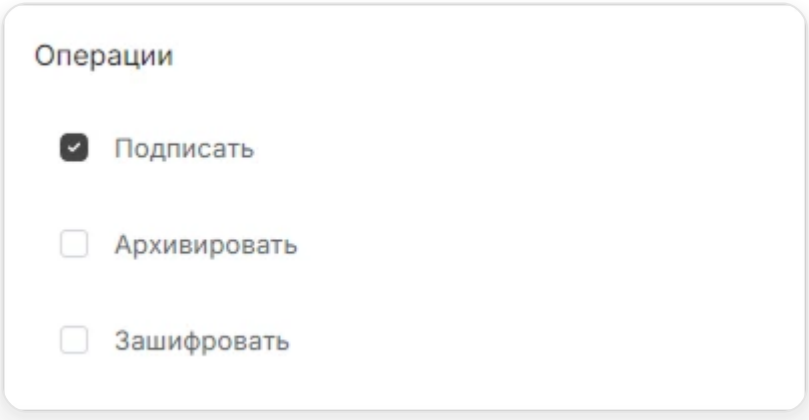
1. Перетащите один или несколько файлов в окно приложения,
2. Загрузите с помощью кнопки **Загрузить с компьютера** или **Добавить из Архива**.

> 💡 **Совет**: Вы можете перетаскивать в мастер не только файлы, но и папки. При этом все файлы из вложенных папок также будут добавлены в мастер.

Шаг 3. Настройка параметров подписи

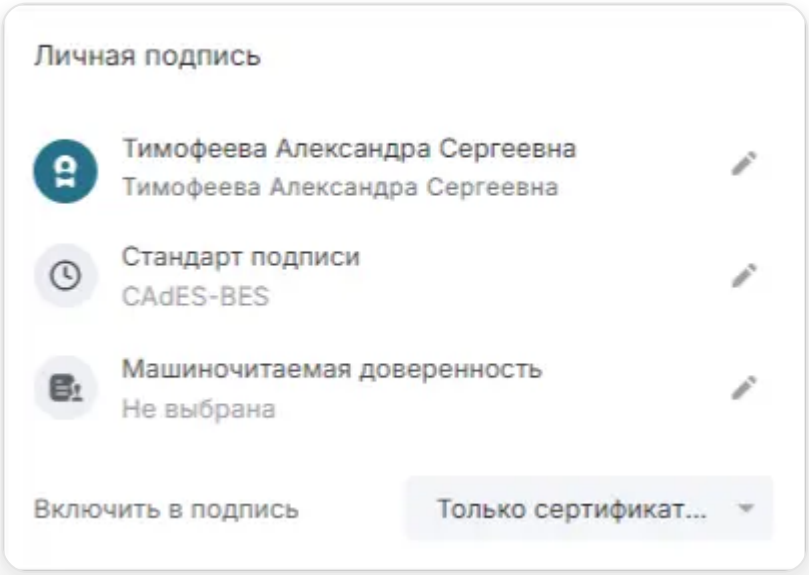
> 💡 **Совет**: По умолчанию в мастере применяются настройки из активного профиля подписи. Вы можете переключаться между профилями, предварительно настроив в каждом нужные параметры для разных операций.

1. Выберите **Подписать** в блоке **Операции**.

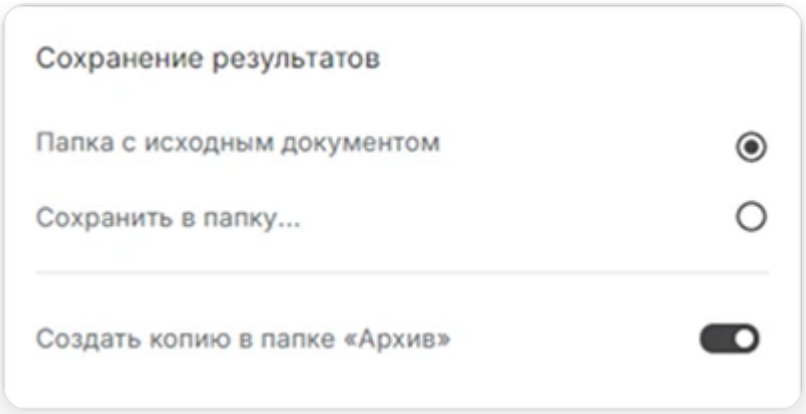


2. В блоке **Личная подпись** выберите:
    - **Личный сертификат**. Нажмите на кнопку **Редактировать** и в открывшемся окне кликните на иконку нужного сертификата. При необходимости можно просмотреть сведения о сертификате по кнопке .

- **Стандарт подписи**. Нажмите на кнопку **Редактировать** и в открывшемся окне выберите один из доступных стандартов. Для стандартов со штампами потребуется указать дополнительные настройки служб штампов времени. Подробнее читайте в инструкции Настройки для стандартов со штампами.
- **Машиночитаемую доверенность** (при необходимости). Файлы доверенности будут сохранены в папку с подписанным файлом.



3. При необходимости внесите изменения в дополнительные настройки, скрытые в кнопку **Дополнительно**.
4. Укажите настройки для сохранения результата операции.



5. Нажмите кнопку **Выполнить**.

Шаг 4. Подтверждение операции

Перед выполнением подписи запрашивается ее подтверждение.

Чтобы подтвердить операцию:

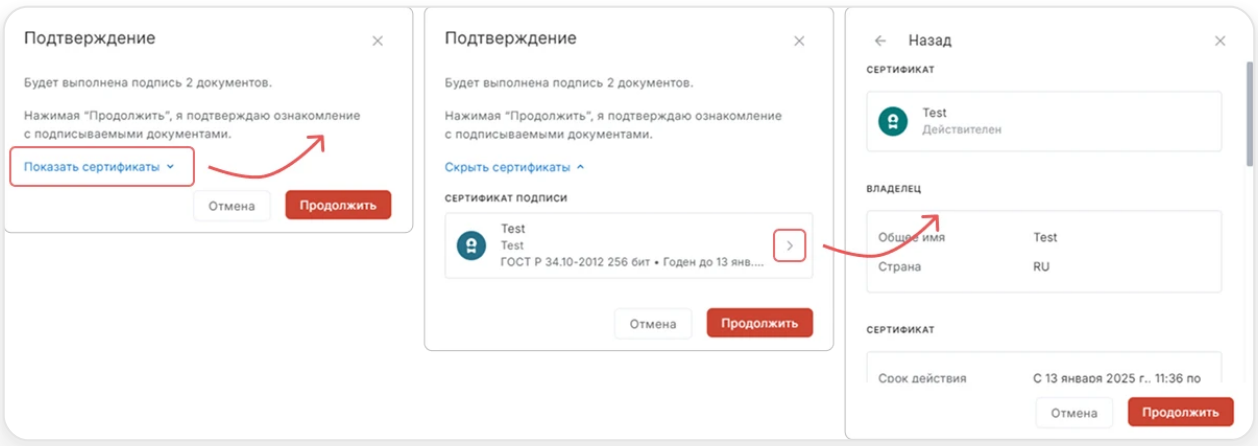
1. Ознакомьтесь со сведениями в окне **Подтверждение**. Окно содержит сведения о количестве документов и выполняемой с ними операции, а также сертификатах, которые будут использоваться.

2. Нажмите кнопку **Продолжить**.

   Нажав «Продолжить» в окне, вы подтверждаете, что ознакомились с подписываемыми данными.

После подтверждения будет запущено выполнение операции.

> 💡 **Совет**: Чтобы просмотреть информацию о сертификате подписи, нажмите на кнопку **Показать сертификат**. После этого нажмите на панель с сертификатом.

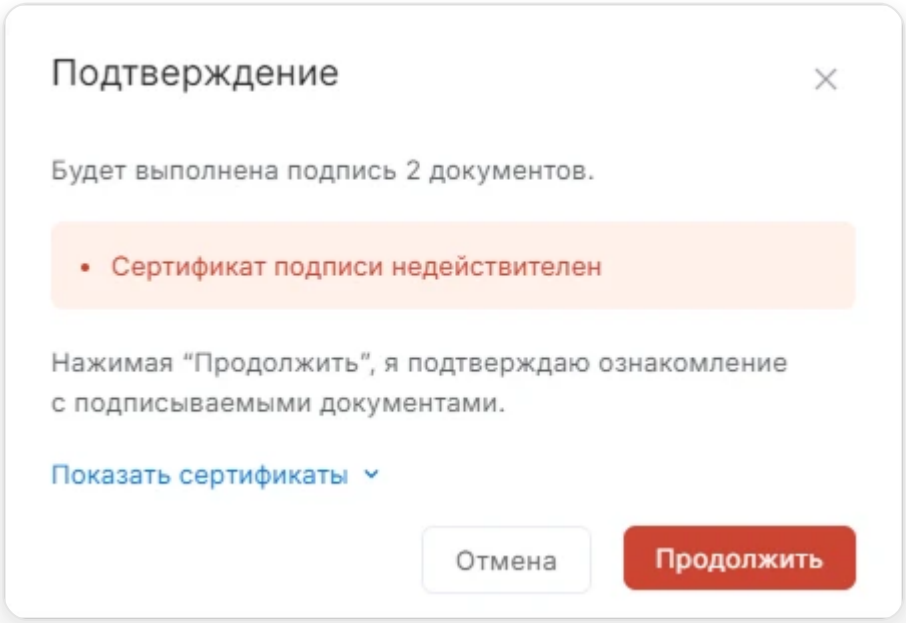


> 💡 **Совет**: Чтобы отменить операцию, нажмите на кнопку «Отмена». Следует помнить, что все операции с документами выполняются последовательно, и если вы нажмёте на кнопку, то операция будет остановлена на том документе, с которым производилась на момент отмены.

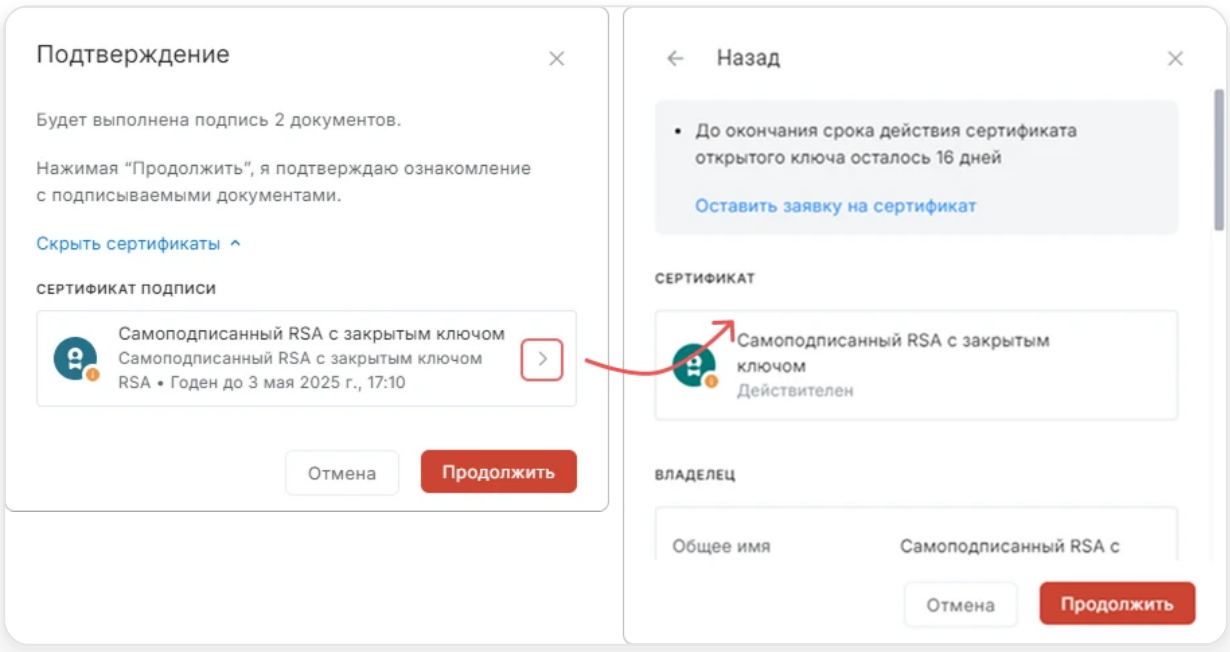
Дополнительные уведомления

В окне с подтверждением операции могут появиться дополнительные уведомления, если:

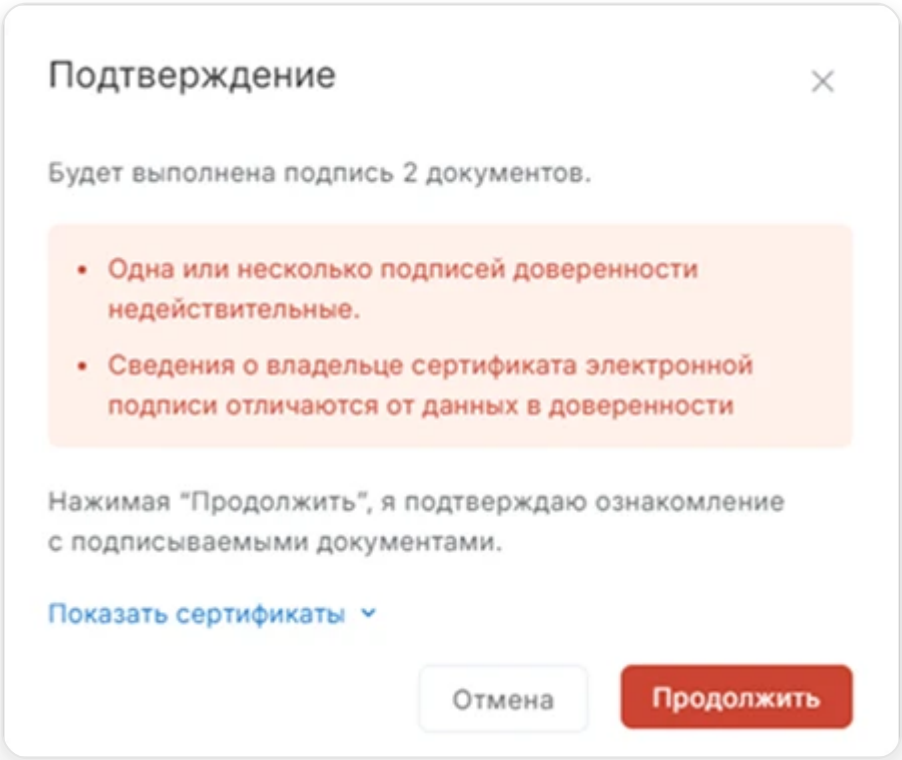
- Сертификат подписи недействителен,



- Срок действия открытого или закрытого ключа личного сертификата 30 дней и менее,



- Сертификат подписи машиночитаемой доверенности недействительный или сведения о владельце сертификата подписи отличаются от данных в машиночитаемой доверенности.



🚨 **Важно**: Во всех случаях подпись будет выполнена, но стоит учесть, что её действительность может быть поставлена под сомнение.

Шаг 5. Результат операции

Если операция прошла успешно, подписанные файлы будут сохранены в соответствии с указанными настройками.

💡 В окне с результатами операции вы можете ознакомиться с информацией о подписи, отправить файл по электронной почте, сохранить его в «Архиве» и многое другое. Подробнее читайте в инструкции Действия с документами.

Подписание сертификатом DSS

Особенности

Сертификат DSS — сертификат электронной подписи, ключ от которого генерируется и хранится на сервере Удостоверяющего центра. Благодаря этому владельцу сертификата не требуется записывать и хранить ключ на токене или компьютере. Это позволяет ему подписывать электронные документы с любого устройства и из любого места, где есть доступ в интернет.

Подпись документов с помощью сертификата DSS имеет следующие особенности:

1. **Ограниченные настройки подписи**:
    - Недоступен выбор стандарта подписи PAdES,
    - Отсутствует возможность установки штампов времени.
2. **Процесс аутентификации**:
    - Нужен доступ к интернету,
    - Иногда требуются дополнительные методы подтверждения.

Подпись документов сертификатом DSS

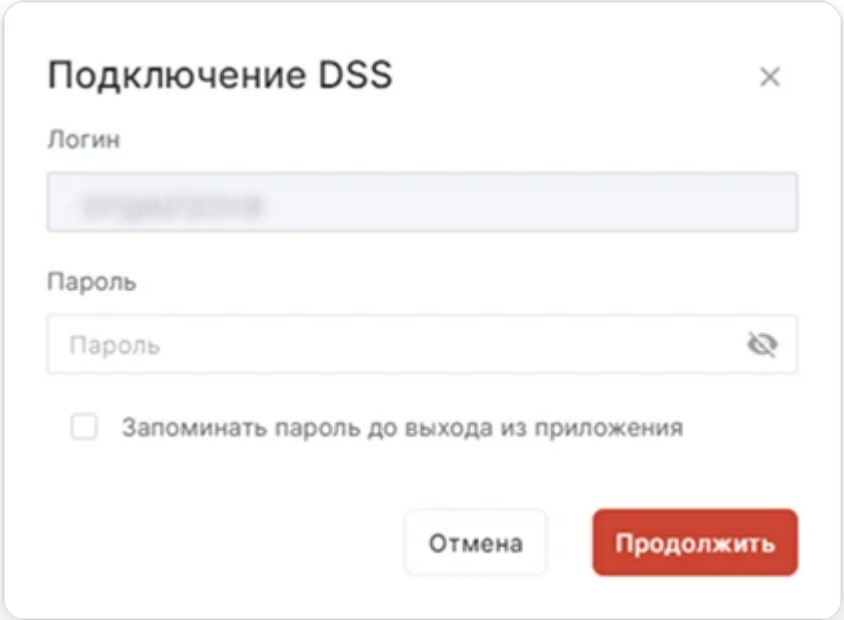
> ⚠️ **Примечание**: Для DSS подписи не требуется лицензия на программный продукт КриптоПро CSP.

Процесс подписи с использованием сертификата DSS не отличается от подписи с помощью обычного сертификата, за исключением нескольких шагов.

1. Добавьте документы в мастер.
2. Выберите **Подписать** в блоке **Операции**.
3. Выберите DSS-сертификат в блоке **Личная подпись**.
4. Укажите настройки для сохранения результата и нажмите на кнопку **Выполнить**:
5. При необходимости пройдите аутентификацию в DSS-сервисе:
    - Может быть открыто окно для ввода пароля для аутентификации на сервисе DSS, если для аутентификации задан пароль и время действия токена аутентификации истекло.

      Введите пароль и нажмите **Продолжить**.

      Если токен аутентификации не истек, то данный шаг пропускается.

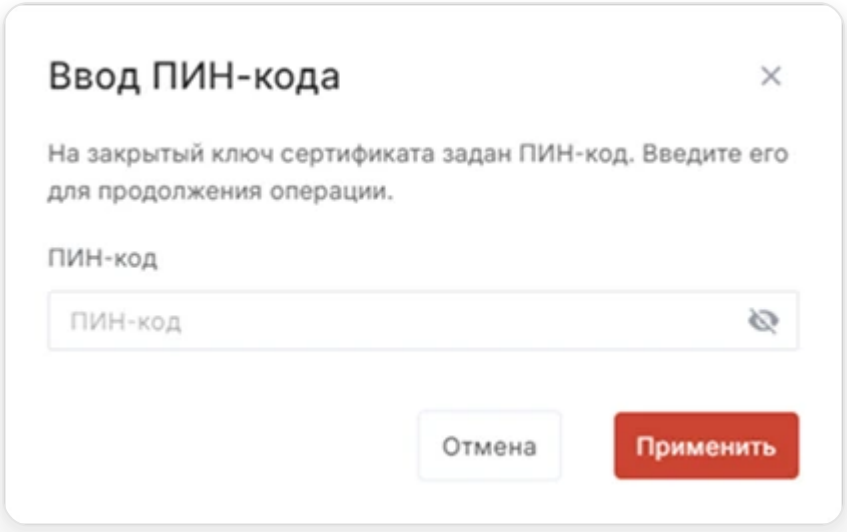


- Может быть открыто окно для подтверждения аутентификации на сервисе DSS, если для аутентификации задан вход по SIM-карте или по мобильному приложению и время действия токена аутентификации истекло. Подтвердите операцию входа на сервис на устройстве. Если токен аутентификации не истек, то данный шаг пропускается.

6. При необходимости укажите пароль к ключевому контейнеру.

   Введите пароль и нажмите **Применить**.

   Если пароль не задан, то данный шаг пропускается.



7. Подтвердите операцию на вашем устройстве. У разных DSS-провайдеров могут быть разные способы подтверждения: через SIM-карту или с помощью мобильного приложения.

8. Дождитесь окончания операции.

Возможные ошибки

При возникновении ошибки вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

> ⚠️ **Примечание**: Коды ошибок (0x...) фиксируются для криптопровайдера КриптоПро CSP.

Код ошибки	Ошибка	Рекомендуемые действия
-	**Не удалось открыть файл**	1. Проверьте наличие и доступность файлов 2. Убедитесь, что файлы не пустые (имеют ненулевой размер) 3. Повторите добавление файлов в мастер
-	**Не удалось подписать файл**	1. Проверьте права доступа к папке, указанной для сохранения результатов 2. Освободите место на диске
-	**Отсутствует необходимый криптопровайдер. Алгоритм открытого ключа сертификата: ГОСТ Р 34.10-2012 256 бит**	Установите криптопровайдер КриптоПро CSP и перезапустите приложение КриптоАРМ
-	**Отсутствует действующая лицензия КриптоАРМ**	1. Приобретите лицензию КриптоАРМ 2. Активируйте лицензию в настройках программы
0x8009001d	**Отсутствует действующая лицензия КриптоПро CSP**	Установите лицензию КриптоПро CSP
0xc2100140	**Отсутствует лицензия на модуль КриптоПро TSP Client**	Приобретите и установите лицензию TSP Client
0xc2110140	**Отсутствует лицензия на модуль КриптоПро OCSP Client**	Приобретите и установите OCSP Client
-	**Не установлены модули TSP/ OCSP Client**	Установите недостающие модули
-	**Не выбран сертификат подписи**	Выберите сертификат в настройках подписи
-	**Не указан адрес службы TSP**	Введите корректный адрес TSP-сервера

Код ошибки	Ошибка	Рекомендуемые действия
0x80072ee7	**Некорректный адрес службы TSP**	1. Проверьте правильность введенного адреса 2. Убедитесь в доступности сервера
-	**Сертификат не подходит для усовершенствованной подписи**	Выберите подходящий сертификат или измените настройки стандарта подписи
-	**Не указан адрес прокси-сервера**	1. Введите корректный адрес прокси 2. Проверьте параметры сети
-	**Не указан порт прокси-сервера**	1. Укажите правильный порт прокси-сервера 2. Проверьте настройки подключения
0x80072ee6	**Некорректные настройки прокси**	1. Проверьте параметры прокси-сервера 2. Временно отключите прокси для тестирования
-	**Папка для сохранения не найдена**	1. Проверьте существование указанной папки 2. Создайте и укажите новую папку для результатов
-	**Файл МЧД поврежден или не обнаружен**	1. Проверьте целостность файла машиночитаемой доверенности 2. Запросите корректную версию файла
0x80072ee7	**Нет подключения к интернету**	1. Проверьте сетевое подключение 2. Убедитесь, что брандмауэр не блокирует соединение (Для подписей со штампами)

Инструкции по теме

- Подпись документов со стандартом PAdES
- Добавление соподписи
- Установка личного сертификата
- Создание профиля подписи
- Переключение между профилями подписи
- Проверка подписи документа

Открыть статью на сайте

Подпись со стандартом PAdES

- О подписи PAdES
- Подпись документов
- Настройка положения штампа
- Настройка внешнего вида штампа
- Возможные ошибки

О подписи PAdES

PAdES — это стандарт электронной подписи, созданный для PDF-документов. Его главным преимуществом является встроенная подпись.

Встроенная подпись дает возможность подписывать электронные документы, не изменяя формат файла и не создавая отдельный файл подписи, как это происходит при использовании присоединенной и отсоединенной подписи в рамках стандарта CAdES. Подпись встраивается непосредственно в сам электронный документ, что делает возможным его открытие без специализированного программного обеспечения.

Подпись может быть добавлена в документ как видимая, так и невидимая.

Видимая подпись отображается на странице документа в виде штампа. Невидимая подпись визуально на странице документа не видна. При проверке как видимой, так и невидимой подписи можно получить сведения о статусе подписи и сертификате подписанта.

В КриптоАРМ можно создать электронную подпись файлов со стандартами:

- **PAdES-BES** - базовая подпись без меток времени,
- **PAdES-T** - подпись со штампом времени (TSP) для фиксации момента подписания,
- **PAdES-A** - для создания подписи с архивными штампами времени,
- **PAdES-X Long Type 1** - для создания усовершенствованной подписи. Расширяет стандарт PAdES-A: сохраняет полные доказательства валидации и цепочки сертификатов.

> 💡 **Совет**: С помощью мастера «Подпись и шифрование» вы можете выполнить групповую подпись PDF-файлов со стандартом PAdES. Для подписи одного файла рекомендуется воспользоваться мастером «Подпись и защита PDF».

Подпись документов

> 💡 **С чего начать**: Чтобы оценить, готово ли ваше рабочее место для работы с электронной подписью, воспользуйтесь Проверкой рабочего места.
>
> ⚠️ **Примечание**: Если в списке файлов на подпись будут документы, не относящиеся к формату PDF, то подпись PAdES будет выполнена только для PDF-файлов, а для остальных — подпись со стандартом CAdES.

Шаг 1. Запуск мастера

1. Перейдите в раздел **Документы**.
2. Нажмите **Подпись и шифрование** в боковом меню раздела **Документы**.
3. Откроется новая вкладка с мастером.

> 💡 **Совет**: Открыть мастер можно с помощью действия **Добавить в** → **Подпись и шифрование** для файла в папке «Архив», результатах операции или в разделе «Почта».

Шаг 2. Добавление документов

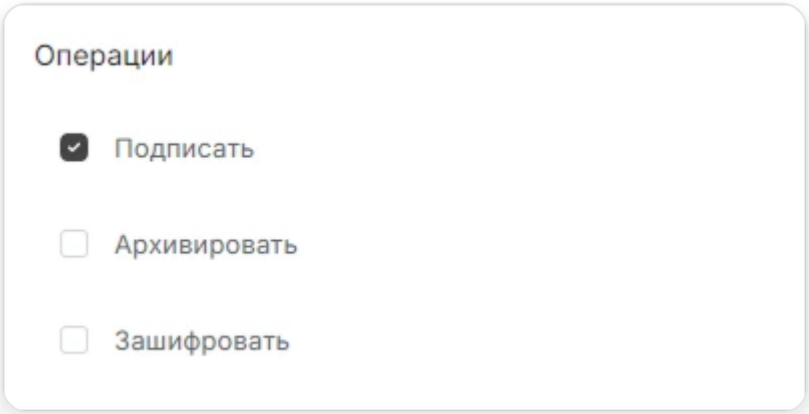
Добавьте документы в мастер одним из способов:

1. Перетащите один или несколько файлов в окно приложения,
2. Загрузите с помощью кнопки **Загрузить с компьютера** или **Добавить из Архива**.

Шаг 3. Настройка параметров подписи

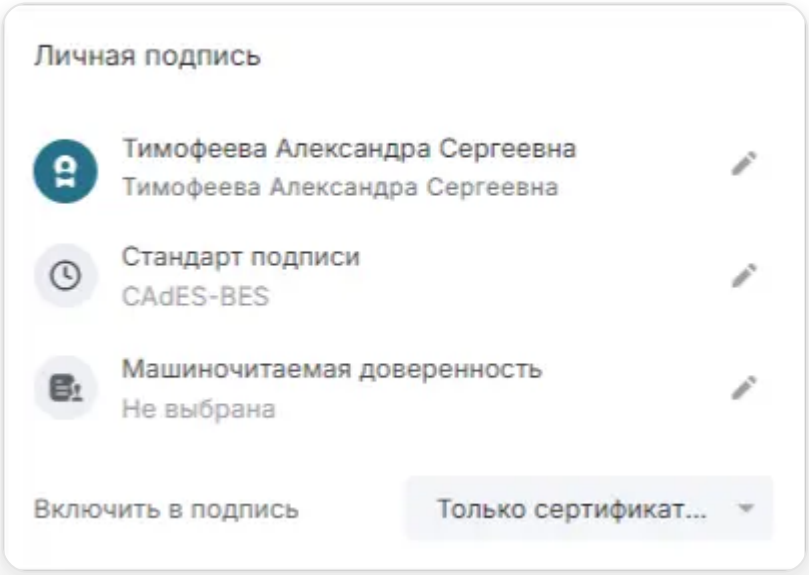
> 💡 **Совет**: По умолчанию в мастере применяются настройки из активного профиля подписи. Вы можете переключаться между профилями, предварительно настроив в каждом нужные параметры для разных операций.

1. Выберите **Подписать** в блоке **Операции**.



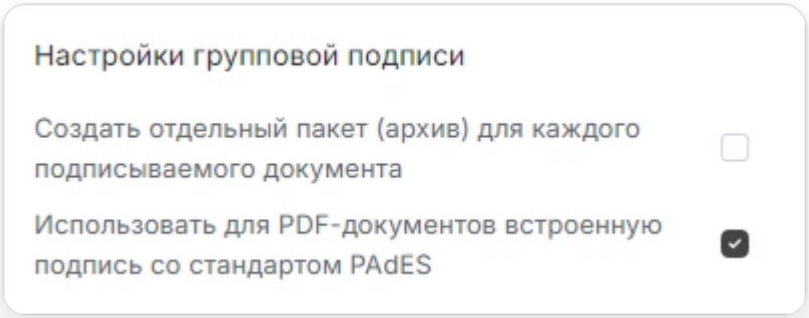
2. В блоке **Личная подпись** выберите:
   - **Личный сертификат**. Нажмите на кнопку **Редактировать** и в открывшемся окне кликните на иконку нужного сертификата. При необходимости можно просмотреть сведения о сертификате по кнопке .
   - **Стандарт подписи**. Нажмите на кнопку **Редактировать** и в открывшемся окне выберите один из доступных стандартов. Для стандартов со штампами потребуется указать дополнительные настройки служб штампов времени. Подробнее читайте в инструкции Настройки для стандартов со штампами.
   - **Машиночитаемую доверенность** (при необходимости). Файлы доверенности будут сохранены в папку с подписанным файлом.

> 🚨 **Важно**: Сертификат DSS не подходит для подписи PDF-файлов со стандартом PAdES.



3. Раскройте дополнительные настройки, скрытые в кнопку **Дополнительно**.

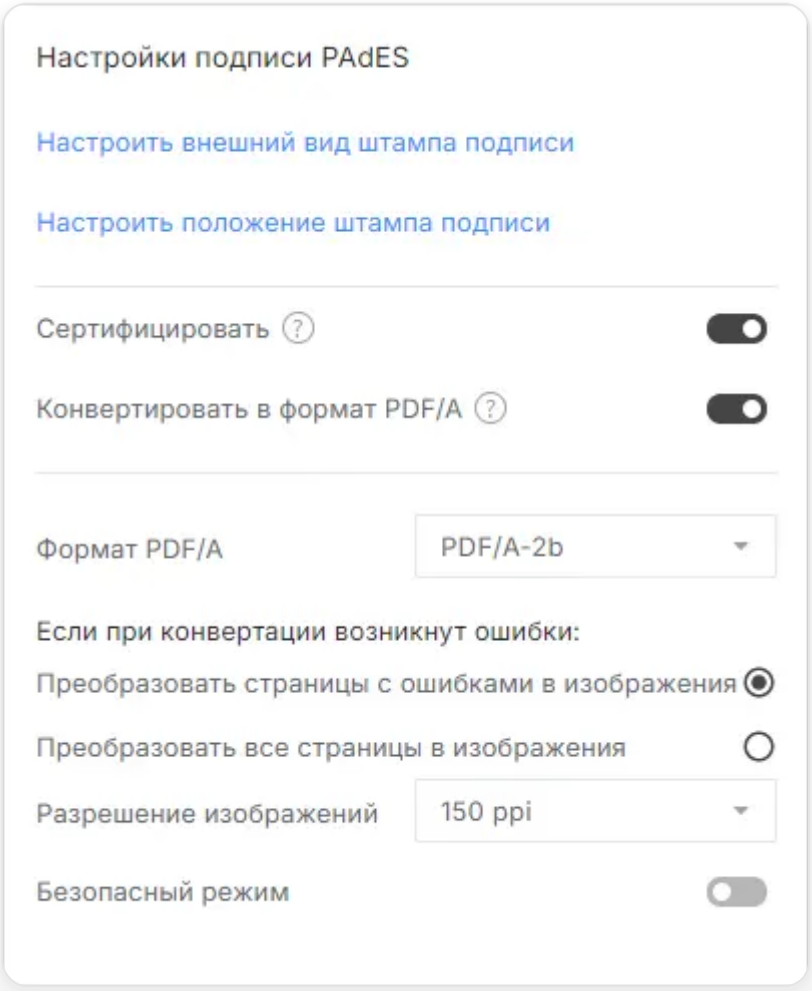
4. В блоке **Настройки групповой подписи** установите флажок для настройки **Использовать для PDF-документов встроенную подпись со стандартом PAdES**.



5. В блоке **Настройки подписи PAdES** настройте:

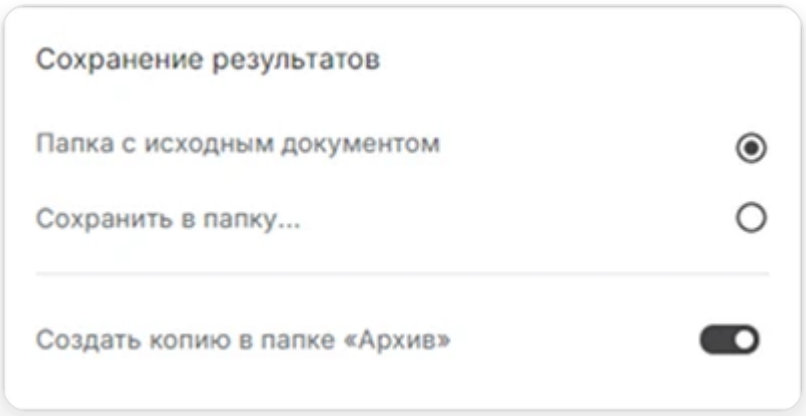
   - Положение штампа подписи,
   - Внешний вид штампа подписи,
   - При необходимости активируйте переключатель **Сертифицировать** для включения режима защиты от изменений.
   - При необходимости активируйте переключатель **Конвертировать в формат PDF/A** для удаления потенциально опасных элементов. Для конвертации потребуется указать дополнительные настройки.

> 🔍 Подробнее читайте в инструкции Настройки защиты PDF-документа.



6. При необходимости внесите изменения в остальные настройки.

7. Укажите настройки для сохранения результата операции.



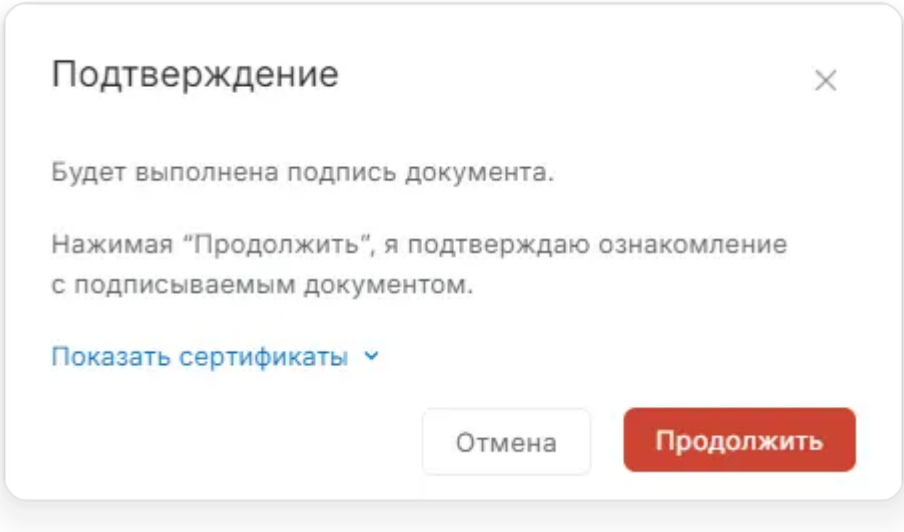
8. Нажмите кнопку **Выполнить**.

Шаг 4. Подтверждение операции

Перед выполнением подписи запрашивается ее подтверждение.

Чтобы подтвердить операцию:

1. Ознакомьтесь со сведениями в окне **Подтверждение**. Окно содержит сведения о количестве документов и выполняемой с ними операции, а также сертификатах, которые будут использоваться.
2. Нажмите кнопку **Продолжить**.



Нажав «Продолжить» в окне, вы подтверждаете, что ознакомились с подписываемыми данными.

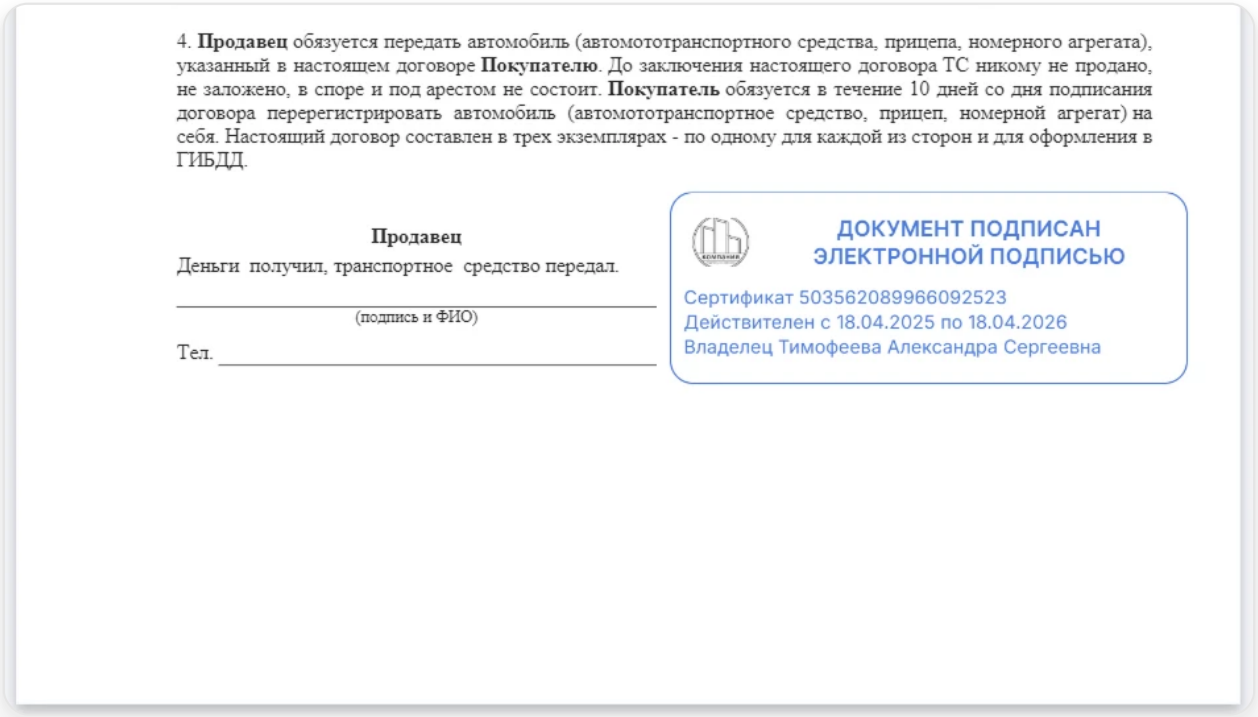
После подтверждения будет запущено выполнение операции.

Шаг 5. Результат операции

Если операция прошла успешно, подписанные файлы будут сохранены в соответствии с указанными настройками.

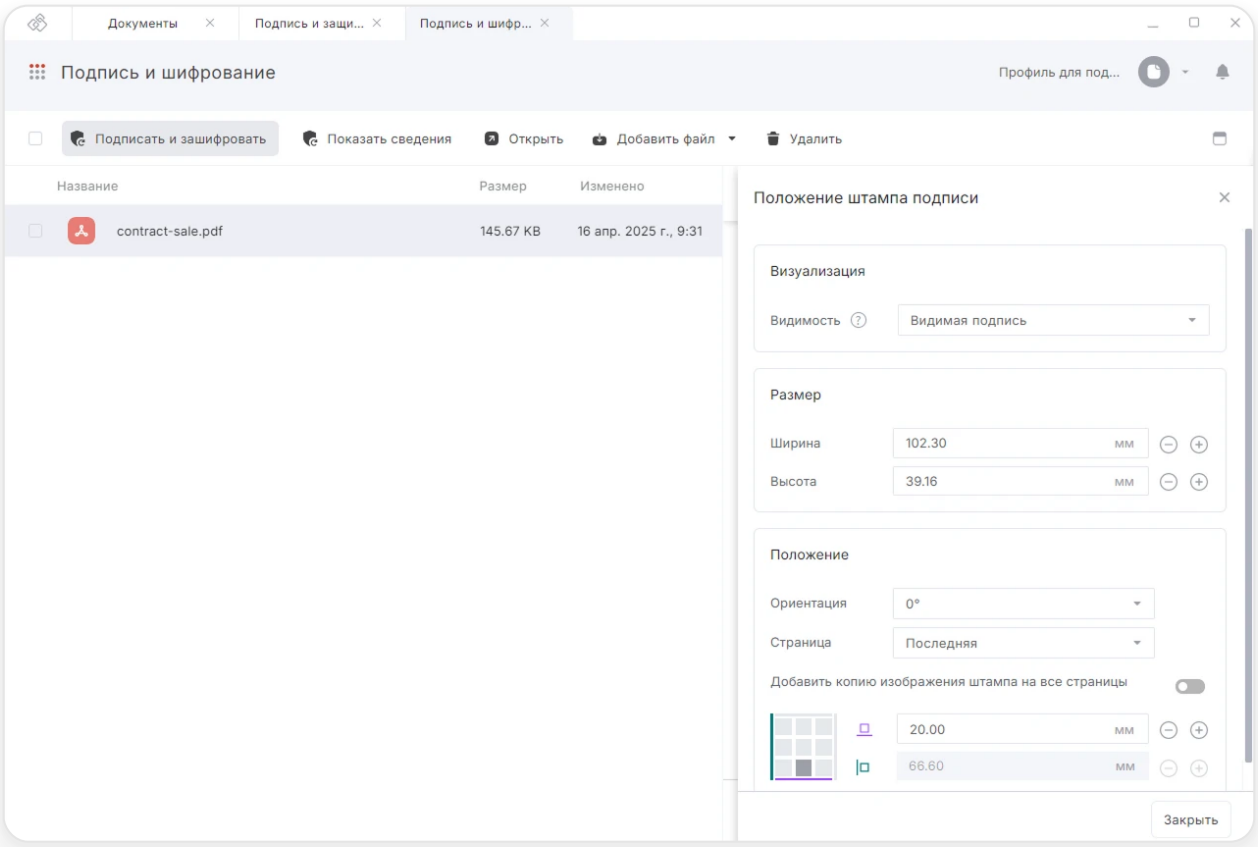
> 💡 В окне с результатами операции вы можете ознакомиться с информацией о подписи, отправить файл по электронной почте, сохранить его в «Архиве» и многое другое. Подробнее читайте в инструкции Действия с документами.

Пример визуализации штампа подписи:



Настройка положения штампа

Откройте окно настроек, нажав на кнопку **Настроить положение штампа подписи** в блоке **Настройки подписи PAdES**.



1. Видимость подписи

Настройте визуальное отображение подписи в блоке **Визуализация**:

- **Видимая подпись** - подпись отображается в документе в виде штампа,
- **Невидимая подпись** - подпись существует, но не видна.

2. Размер штампа

Укажите ширину и высоту штампа в миллиметрах.

> 💡 Задайте параметры штампа в следующих пределах: ширина — от 1 до 207,9 мм, высота — от 1 до 294,69 мм. Эти размеры соответствуют формату страницы A4 и не выходят за его пределы. Важно учесть, что на размер штампа также оказывают влияние значения, указанные в блоке «Положение».

3. Положение штампа

1. Выберите значение для ориентации штампа.
2. Укажите страницу расположение штампа:
    - Последняя - для размещения штампа на последней странице документа,

- Указать страницу - для выбора страницы размещения,
- При необходимости активируйте переключатель **Добавить копию изображения штампа на все страницы**.

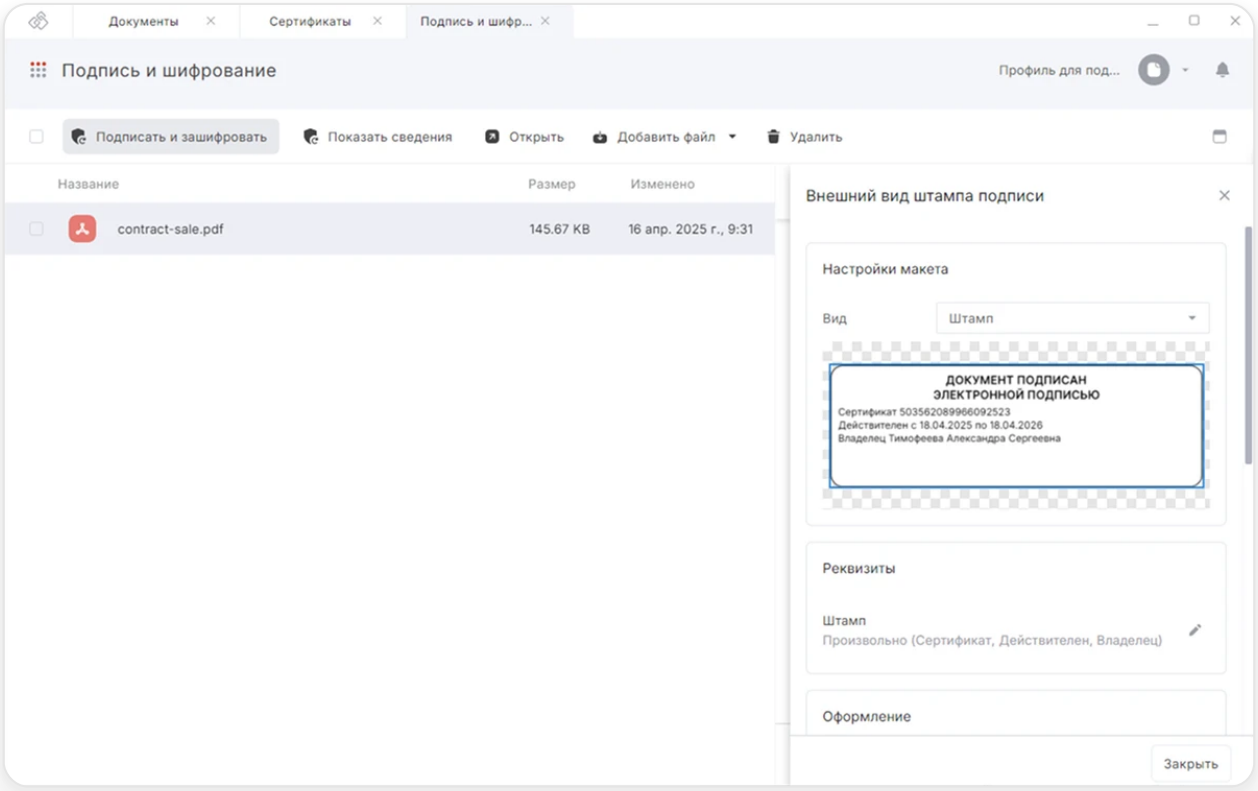
3. Настройте размещение штампа:

   - Задайте способ выравнивания,
   - Укажите координаты (X,Y).

Настройка внешнего вида штампа

Откройте окно настроек:

1. Нажмите на кнопку **Настроить внешний вид штампа подписи** в блоке **Настройки подписи PAdES**.
2. Откроется окно с настройками, в котором доступен предварительный просмотр штампа.

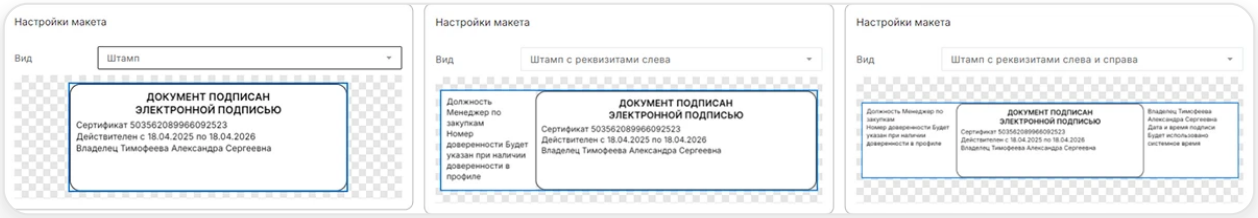


1. Вид штампа

Выберите макет штампа в настройке **Вид**:

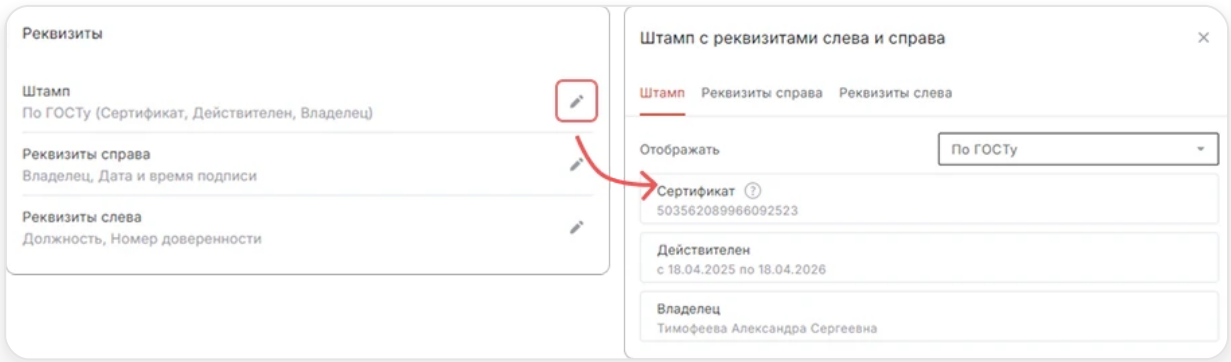
- **Штамп** - в области будет размещен только штамп.
- **Штамп с реквизитами слева** - в области будет размещен штамп, а также блок с реквизитами слева от штампа.

- **Штамп с реквизитами справа** - в области будет размещен штамп, а также блок с реквизитами справа от штампа.
- **Штамп с реквизитами слева и справа** - в области будет размещен штамп, а также блок с реквизитами слева и справа от штампа.

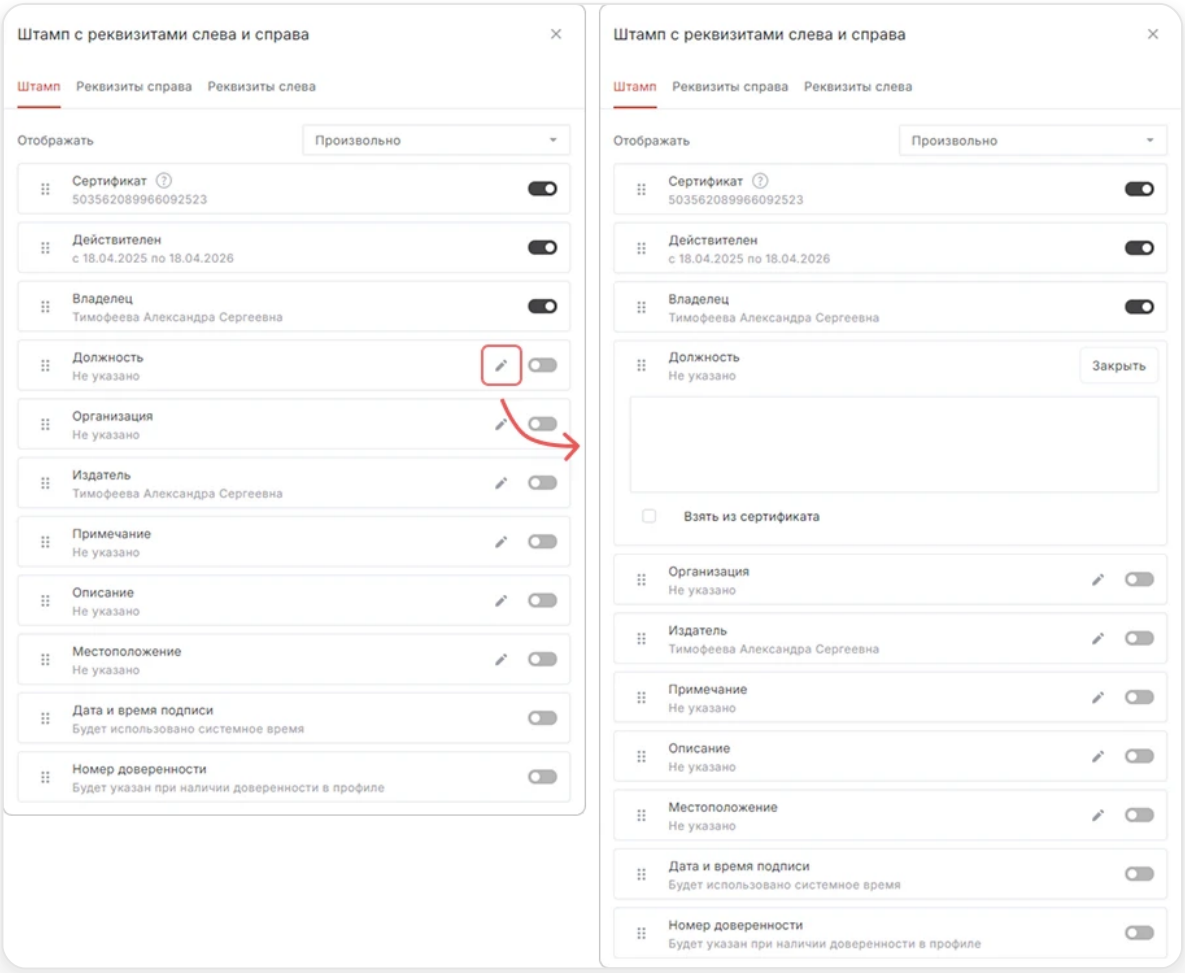


2. Настройка реквизитов

1. Нажмите на кнопку **Редактировать** в блоке **Реквизиты**.
2. В открывшемся окне укажите настройки отображения:
   - **По ГОСТу** - для вывода реквизитов в соответствии с **ГОСТ Р 7.0.97-2016** (Заголовок «Документ подписан электронной подписью», а также серийный номер сертификата, имя его владельца и срок действия).



   - **Произвольно** - для самостоятельной настройки реквизитов.
     - Активируйте переключатели нужных реквизитов.
     - При необходимости измените порядок отображения реквизитов с помощью кнопки . Наведите курсор мыши на кнопку и, удерживая левую кнопку мыши на кнопке, переместите реквизит в необходимое место в списке.
     - При необходимости настройте значения реквизитов. По умолчанию они берутся из сертификата подписи. Чтобы указать свои значения, нажмите на кнопку **Редактировать**, расположенную на панели с реквизитом. Снимите флажок **Взять из сертификата** и введите новое значение в соответствующее поле.

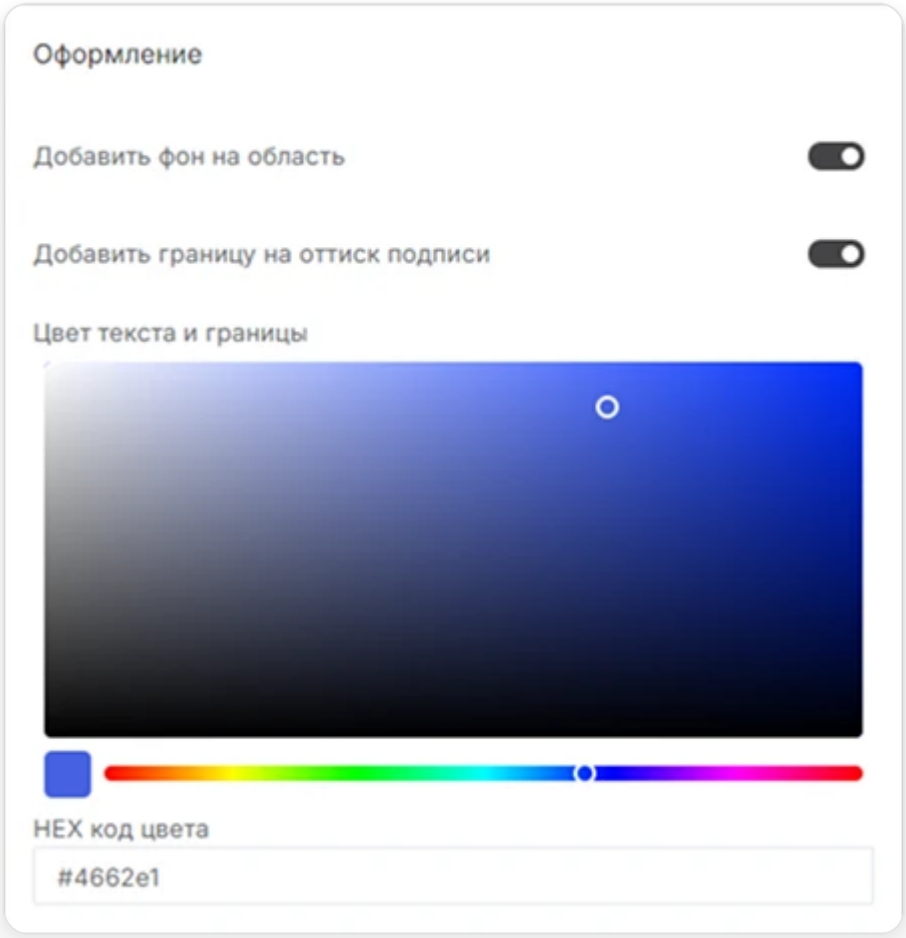


3. Аналогичным образом настройте вывод реквизитов для блоков слева или справа от штампа, если их отображение активировано.

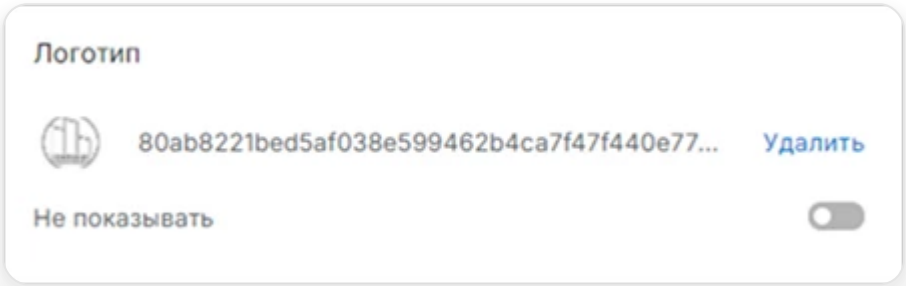
> 💡 **Примечание:** По умолчанию в поле **Владелец** штампа отображается значение **Общее имя (CN)** из сертификата. Если в сертификате указано название организации, а требуется вывести ФИО подписанта, откройте **Настройки визуализации** → **Внешний вид** → **Редактировать** в блоке «Реквизиты», выберите тип штампа «Произвольно» и включите переключатель «ФИО».

3. Оформление

1. Активируйте переключатель **Добавить фон на область** для добавления фона с цветом: #ffffff (hex).
2. Активируйте переключатель **Добавить границу на оттиск подписи** для добавления границы.
3. Настройте цвет границы и текста одним из способов:
   - Выберите необходимый цвет в палитре,
   - Укажите код цвета в hex-формате



4. Загрузите изображение с гербом или эмблемой в блоке **Логотип**.
    - Нажмите на кнопку **Загрузить**,
    - Укажите путь к файлу в окне файлового менеджера.



Возможные ошибки

При возникновении ошибки вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ниже приведены наиболее частые ошибки при работе с PDF-документами. Полный перечень доступен в инструкции.

Ошибка	Описание	Рекомендуемые действия
Не удалось подписать файл: Страница не найдена	Указанный номер страницы для размещения штампа подписи отсутствует в документе	1. Проверьте общее количество страниц в PDF 2. Укажите существующий номер страницы (например, `1` или `последняя`)
Не удалось подписать файл	Возможно, размер или координаты штампа превышают допустимые границы документа	1. Уменьшите размер штампа в настройках 2. Сдвиньте его ближе к центру страницы
Не удалось подписать файл	Возможно, файл имеет ограничения на редактирование, чтение или подпись	1. Запросите у отправителя пароль для снятия защиты 2. Попросите предоставить незащищенную версию
Не удалось подписать сертифицированный документ	Файл уже содержит сертифицирующую подпись, запрещающую дальнейшие изменения	1. Запросите у владельца исходную (не сертифицированную) версию 2. Используйте альтернативный метод подписания (например, внешняя подпись)

Инструкции по теме

- Подпись документа со стандартом CAdES
- Добавление соподписи
- Установка личного сертификата
- Создание профиля подписи
- Переключение между профилями подписи
- Проверка подписи документа

Открыть статью на сайте

Подпись с созданием печатной формы

- Что такое печатная форма
- Подпись документов
- Настройка положения штампа
- Настройка внешнего вида штампа
- Возможные ошибки

Что такое печатная форма

Печатная форма - копия исходного документа с графическим штампом подписи. В такой копии присутствует только визуальное представление штампа, а сама электронная подпись отсутствует.

Важно понимать! Печатная форма документа предназначена для визуального ознакомления с его содержанием и подтверждения факта подписания. Однако она не имеет юридической силы оригинала, поскольку не содержит электронной подписи и связанных с ней криптографических данных.

> 🚨 В текущей версии КриптоАРМ можно создавать печатные формы только для PDF-документов. Эта функция доступна при подписании и просмотре сведений о подписи.

Подпись документов

> 💡 **С чего начать**: Чтобы оценить, готово ли ваше рабочее место для работы с электронной подписью, воспользуйтесь Проверкой рабочего места.

Шаг 1. Запуск мастера

1. Перейдите в раздел **Документы**.
2. Нажмите **Подпись и шифрование** в боковом меню раздела **Документы**.
3. Откроется новая вкладка с мастером.

> 💡 **Совет**: Открыть мастер можно с помощью действия **Добавить в** → **Подпись и шифрование** для файла в папке «Архив», результатах операции или в разделе «Почта».

Шаг 2. Добавление документов

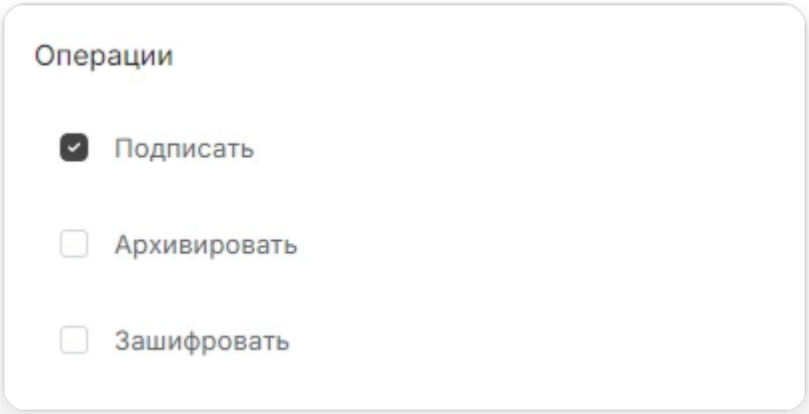
Добавьте документы в мастер одним из способов:

1. Перетащите один или несколько файлов в окно приложения,
2. Загрузите с помощью кнопки **Загрузить с компьютера** или **Добавить из Архива**.

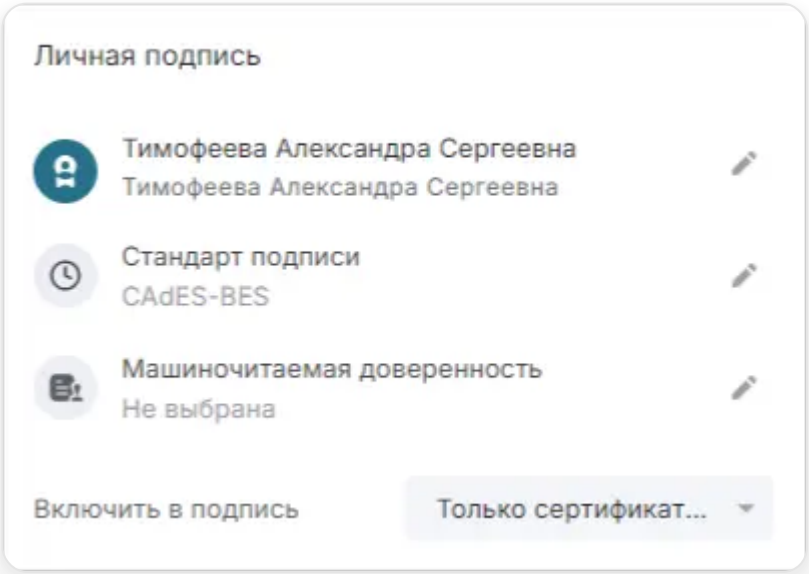
> 💡 **Совет**: Вы можете добавлять документы с любыми расширениями, однако печатная форма будет создана только для PDF-документов.

Шаг 3. Настройка параметров подписи

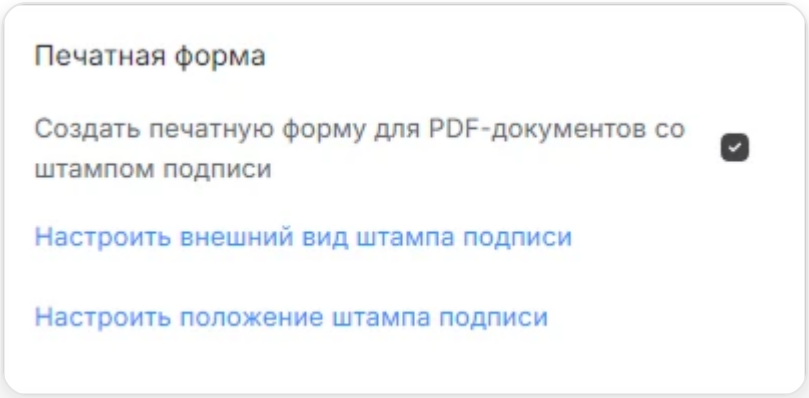
1. Выберите **Подписать** в блоке **Операции**.



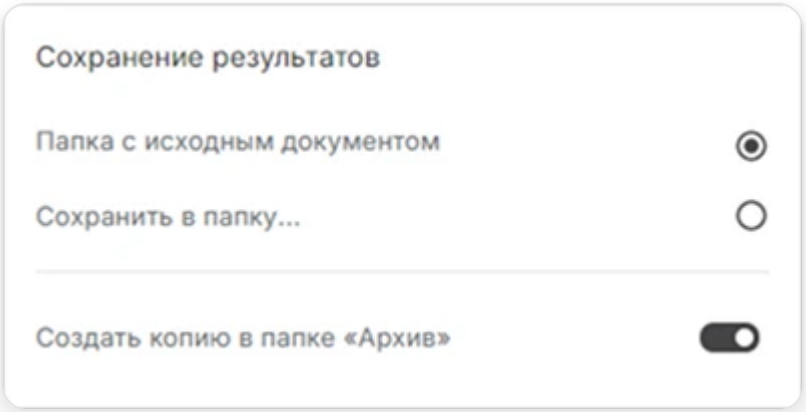
2. В блоке **Личная подпись** выберите:
    - **Личный сертификат**. Нажмите на кнопку **Редактировать** и в открывшемся окне кликните на иконку нужного сертификата. При необходимости можно просмотреть сведения о сертификате по кнопке .
    - **Стандарт подписи**. Нажмите на кнопку **Редактировать** и в открывшемся окне выберите один из доступных стандартов. Для стандартов со штампами потребуется указать дополнительные настройки служб штампов времени. Подробнее читайте в инструкции Настройки для стандартов со штампами.
    - **Машиночитаемую доверенность** (при необходимости). Файлы доверенности будут сохранены в папку с подписанным файлом.



3. Раскройте дополнительные настройки, скрытые в кнопку **Дополнительно**.
4. В блоке **Печатная форма** установите флажок для настройки **Создать печатную форму для PDF-документов со штампом подписи** и настройте:
   - Положение штампа подписи,
   - Внешний вид штампа подписи.



5. При необходимости внесите изменения в остальные настройки.
6. Укажите настройки для сохранения результата операции.



7. Нажмите кнопку **Выполнить**.

Шаг 4. Подтверждение операции

Перед выполнением подписи запрашивается ее подтверждение.

Чтобы подтвердить операцию:

1. Ознакомьтесь со сведениями в окне **Подтверждение**. Окно содержит сведения о количестве документов и выполняемой с ними операции, а также сертификатах, которые будут использоваться.
2. Нажмите кнопку **Продолжить**.

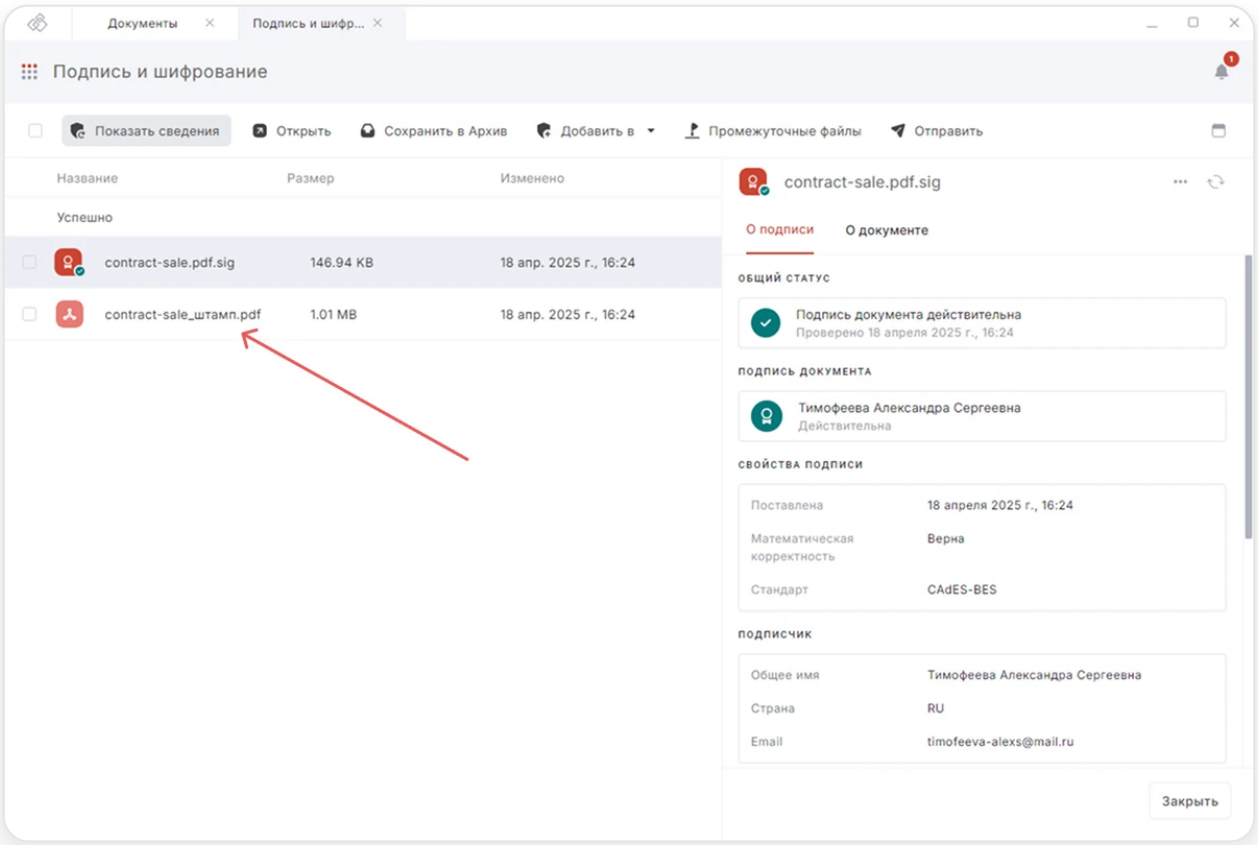
   Нажав «Продолжить» в окне, вы подтверждаете, что ознакомились с подписываемыми данными.

После подтверждения будет запущено выполнение операции.

Шаг 5. Результат операции

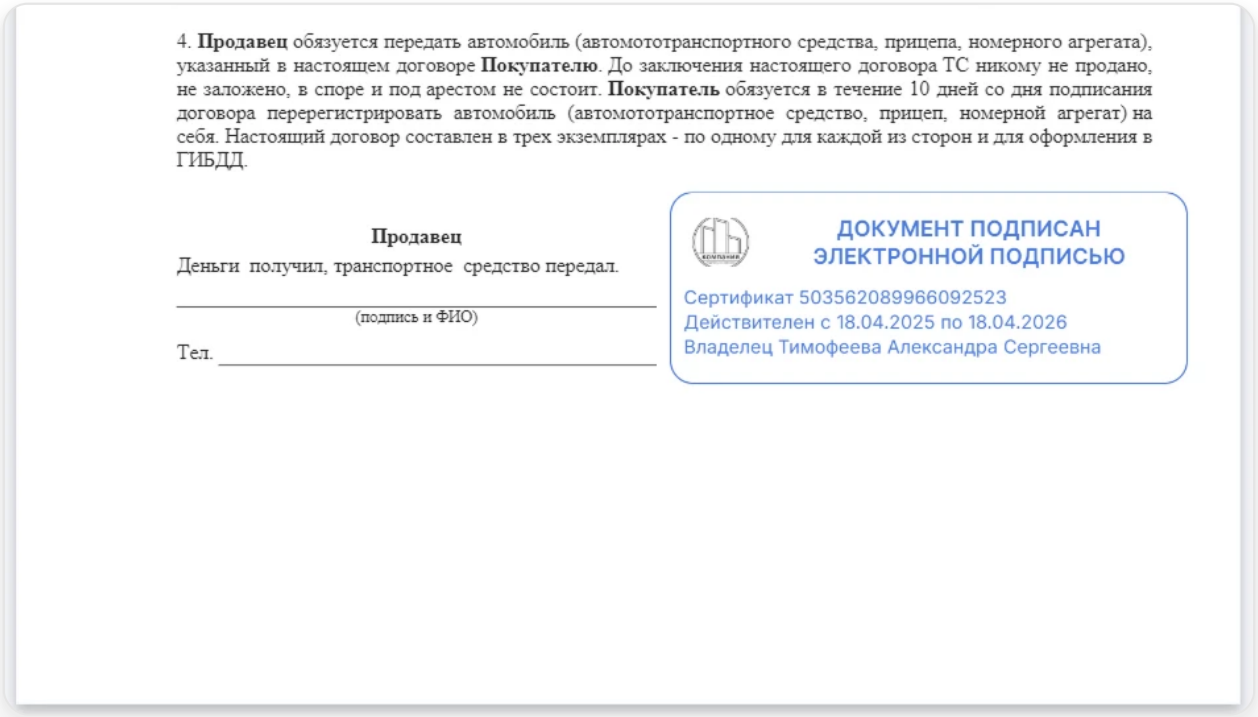
Если операция прошла успешно, подписанные файлы вместе с печатными формами будут сохранены в соответствии с указанными настройками.

В названия файлов с печатными формами будет добавлен текст "_штамп".



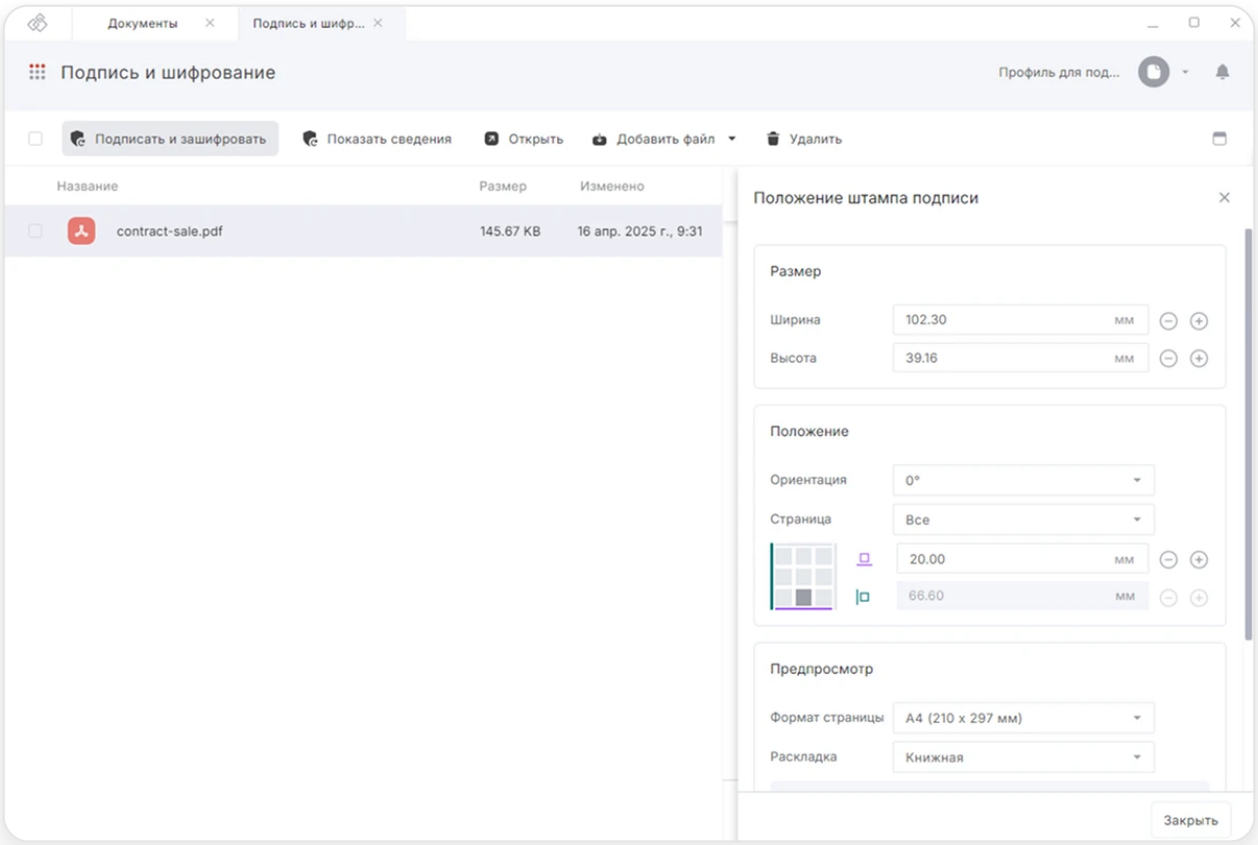
> 💡 В окне с результатами операции вы можете ознакомиться с информацией о подписи, отправить файл по электронной почте, сохранить его в «Архиве» и многое другое. Подробнее читайте в инструкции Действия с документами.

Пример визуализации штампа подписи:



Настройка положения штампа

Откройте окно настроек, нажав на кнопку **Настроить положение штампа подписи** в блоке **Печатная форма**.



1. Размер штампа

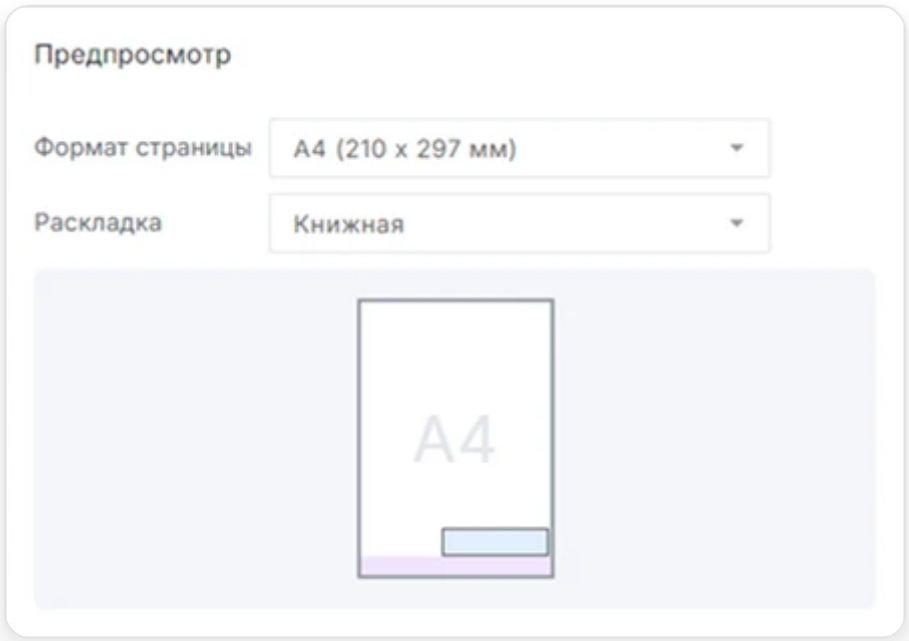
Укажите ширину и высоту штампа в миллиметрах.

> 💡 Задайте параметры штампа в следующих пределах: ширина — от 1 до 207,9 мм, высота — от 1 до 294,69 мм. Эти размеры соответствуют формату страницы A4 и не выходят за его пределы. Важно учесть, что на размер штампа также оказывают влияние значения, указанные в блоке «Положение».

2. Положение штампа

1. Выберите значение для ориентации штампа.
2. Укажите страницу расположение штампа:
    - Все - для размещения штампа на каждой странице документа,
    - Последняя - для размещения штампа на последней странице документа,
    - Некоторые - для указания страниц размещения. Пример заполнения: 1, 5-8, 10.
3. Настройте размещение штампа:
    - Задайте способ выравнивания,
    - Укажите координаты (X,Y).

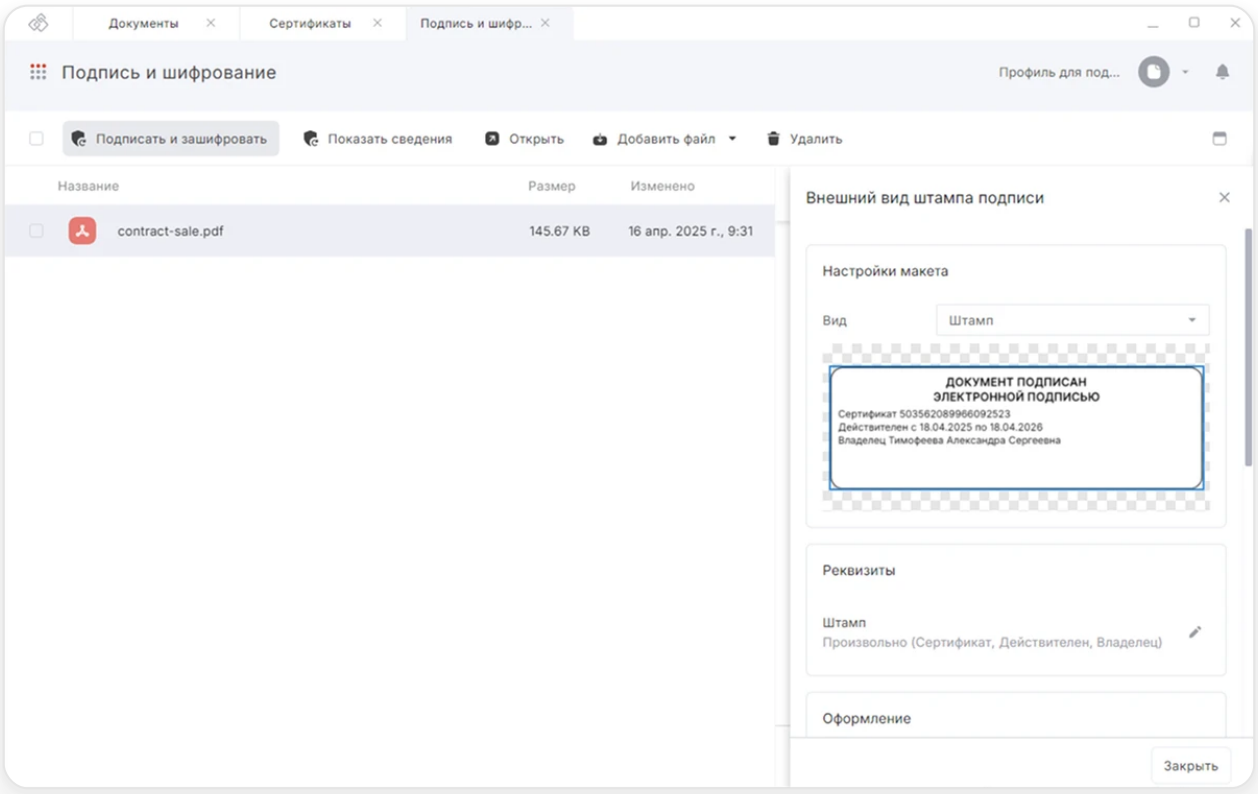
В блоке «Предпросмотр» можно увидеть предварительный просмотр размещения штампа на странице.



Настройка внешнего вида штампа

Откройте окно настроек:

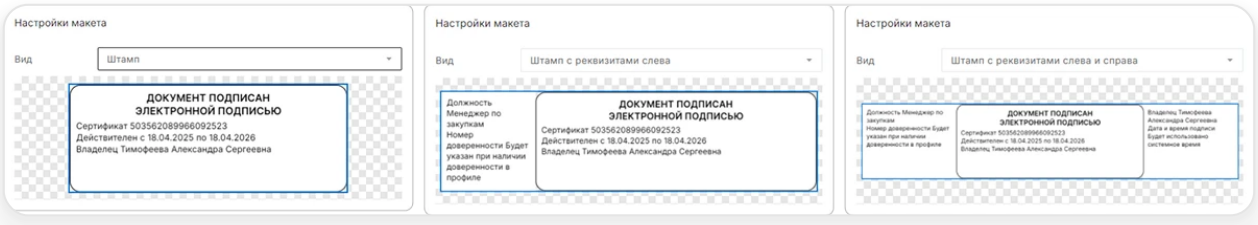
1. Нажмите на кнопку **Настроить внешний вид штампа подписи** в блоке **Печатная форма**.
2. Откроется окно с настройками, в котором доступен предварительный просмотр штампа.



1. Вид штампа

Выберите макет штампа в настройке **Вид**:

- **Штамп** - в области будет размещен только штамп.
- **Штамп с реквизитами слева** - в области будет размещен штамп, а также блок с реквизитами слева от штампа.
- **Штамп с реквизитами справа** - в области будет размещен штамп, а также блок с реквизитами справа от штампа.
- **Штамп с реквизитами слева и справа** - в области будет размещен штамп, а также блок с реквизитами слева и справа от штампа.

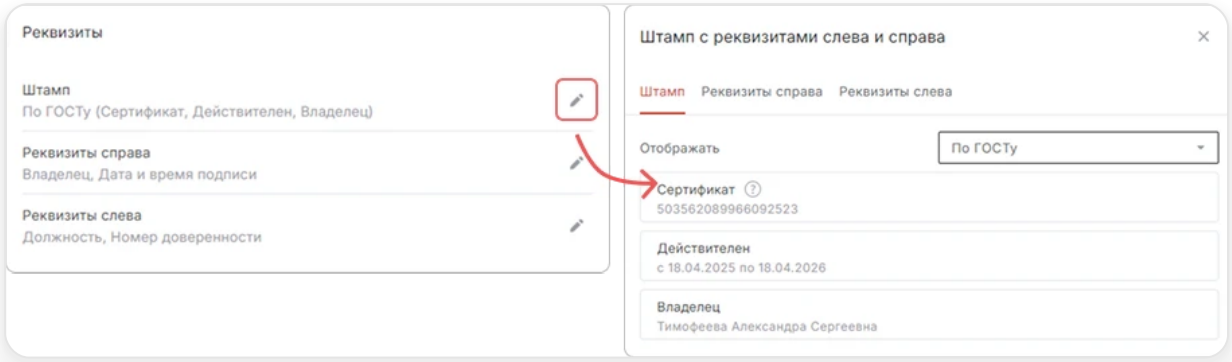


2. Настройка реквизитов

1. Нажмите на кнопку **Редактировать** в блоке **Реквизиты**.

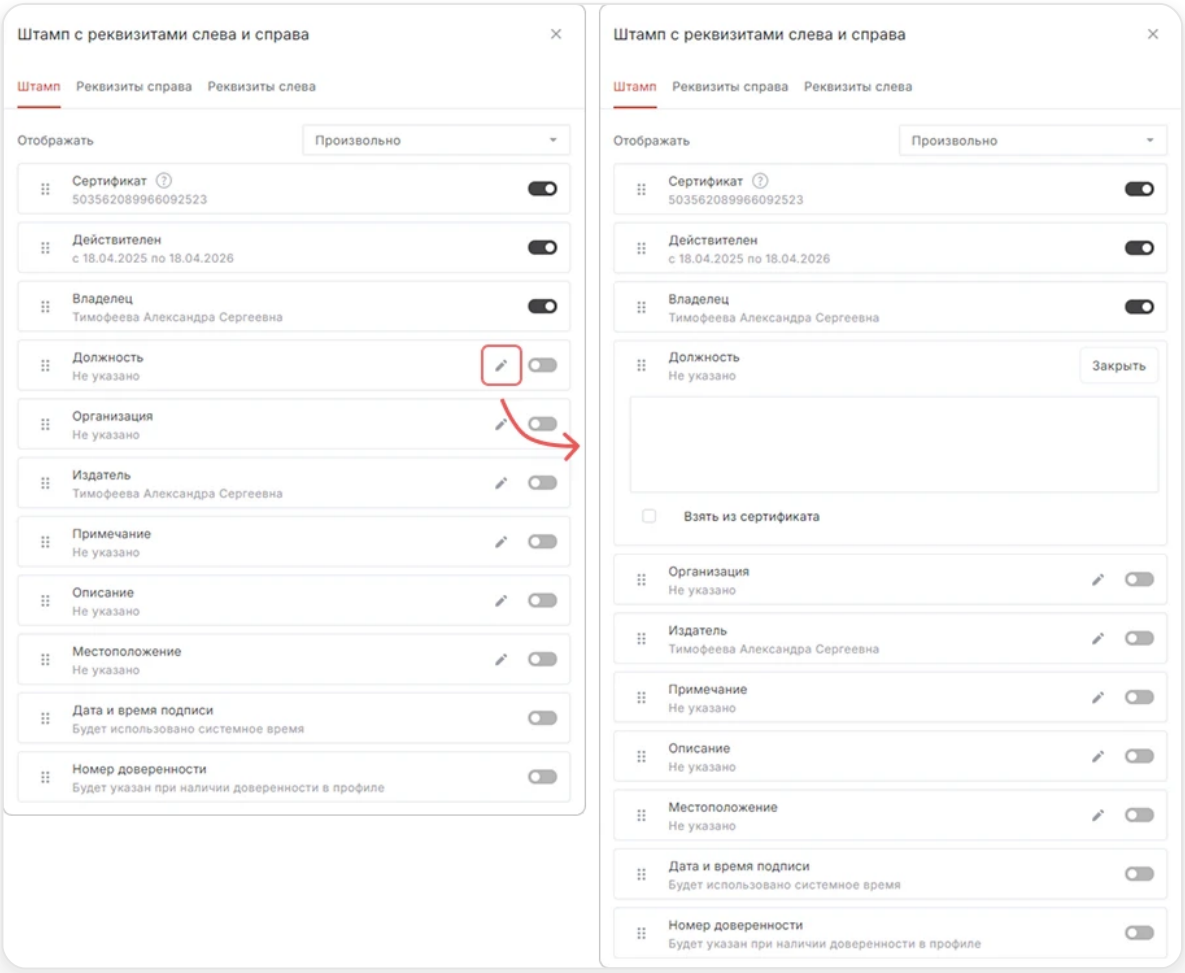
2. В открывшемся окне укажите настройки отображения:

   - **По ГОСТу** - для вывода реквизитов в соответствии с **ГОСТ Р 7.0.97-2016** (Заголовок «Документ подписан электронной подписью», а также серийный номер сертификата, имя его владельца и срок действия).



   - **Произвольно** - для самостоятельной настройки реквизитов.

     - Активируйте переключатели нужных реквизитов.
     - При необходимости измените порядок отображения реквизитов с помощью кнопки ⠿. Наведите курсор мыши на кнопку и, удерживая левую кнопку мыши на кнопке, переместите реквизит в необходимое место в списке.
     - При необходимости настройте значения реквизитов. По умолчанию они берутся из сертификата подписи. Чтобы указать свои значения, нажмите на кнопку **Редактировать**, расположенную на панели с реквизитом. Снимите флажок **Взять из сертификата** и введите новое значение в соответствующее поле.



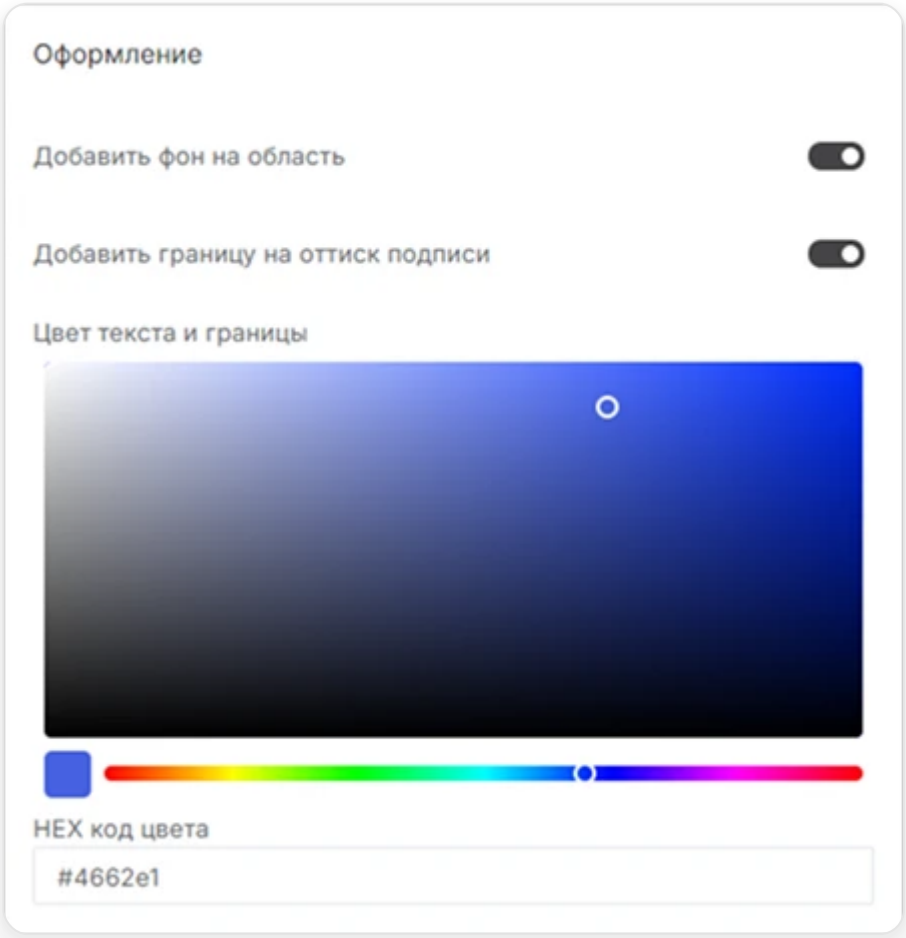
3. Аналогичным образом настройте вывод реквизитов для блоков слева или справа от штампа, если их отображение активировано.

3. Оформление

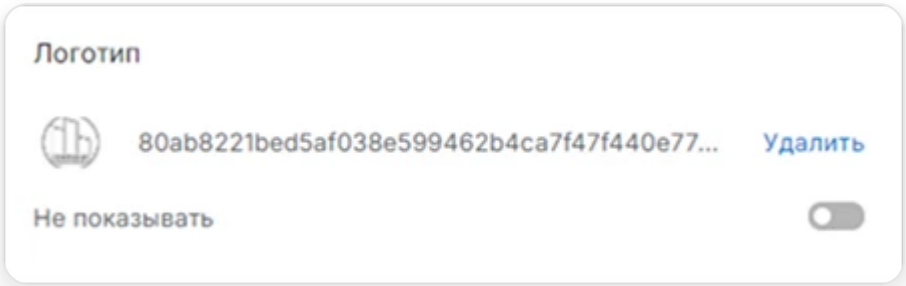
1. Активируйте переключатель **Добавить фон на область** для добавления фона с цветом: #ffffff (hex).
2. Активируйте переключатель **Добавить границу на оттиск подписи** для добавления границы.

3. Настройте цвет границы и текста одним из способов:

    - Выберите необходимый цвет в палитре,
    - Укажите код цвета в hex-формате



4. Загрузите изображение с гербом или эмблемой в блоке **Логотип**.
    - Нажмите на кнопку **Загрузить**,
    - Укажите путь к файлу в окне файлового менеджера.



Возможные ошибки

При возникновении ошибки вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ниже приведены наиболее частые ошибки при работе с печатной формой. Полный перечень доступен в инструкции.

Ошибка	Описание	Рекомендуемые действия
Не удалось подписать файл: Страница не найдена	Указанный номер страницы для размещения штампа подписи отсутствует в документе	1. Проверьте общее количество страниц в PDF 2. Укажите существующий номер страницы (например, `1` или `последняя`)
Не удалось подписать файл	Возможно, размер или координаты штампа превышают допустимые границы документа	1. Уменьшите размер штампа в настройках 2. Сдвиньте его ближе к центру страницы
Не удалось подписать файл	Возможно, файл имеет ограничения на редактирование, чтение или подпись	1. Запросите у отправителя пароль для снятия защиты 2. Попросите предоставить незащищенную версию

Инструкции по теме

- Подпись документа со стандартом CAdES
- Подпись документа со стандартом PAdES
- Добавление соподписи
- Установка личного сертификата
- Создание профиля подписи
- Переключение между профилями подписи
- Проверка подписи документа

Открыть статью на сайте

Добавление соподписи

- Что такое соподпись?
- Как добавить соподпись

Что такое соподпись?

Соподпись - это процесс добавления дополнительной электронной подписи к документу, который уже содержит одну или несколько подписей.

Соподпись может потребоваться в следующих случаях:

- Коллективное утверждение документа;
- Многоэтапное согласование между отделами;
- Подтверждение документа несколькими ответственными лицами.

Особенности соподписи

- Все подписи (первичная и соподписи) имеют равный юридический статус,
- Порядок добавления подписей не влияет на их значимость,
- Каждая подпись содержит полный набор атрибутов (дата, время, сертификат).

> 🚨 **Важно:** Статус документа с соподписями считается действительным в случае действительности всех подписей.

Рекомендации

- **Присоединённая подпись**: если исходный документ содержит присоединённую подпись, рекомендуется делать соподпись также **присоединённой**, чтобы все подписи хранились в одном файле.
- **Отсоединённая подпись**: если исходный документ содержит отсоединённую подпись, соподпись лучше делать **отсоединённой**, чтобы сохранить согласованную схему хранения подписей.

> ⚠️ Несоблюдение согласованного типа подписи может привести к путанице при проверке и хранении документа.

Как добавить соподпись

Процесс добавления соподписи идентичен процедуре первичной подписи документа.

Для выполнения соподписи следуйте инструкциям:

1. Подпись со стандартом CAdES - для группового подписания любых файлов со стандартом CAdES,
2. Подпись со стандартом PAdES - для группового подписания PDF-файлов со стандартом PAdES,
3. Как подписать PDF-документ - для подписания одного PDF-файла со стандартом PAdES.

> 💡 **Совет:** Перед добавлением подписи убедитесь, что исходный документ не был изменён после предыдущего подписания и все предыдущие подписи действительны.
>
> 🚨 **Важно:** Применение различных алгоритмов при соподписи, таких как ГОСТ и RSA, может сделать подпись юридически недействительной.

Инструкции по теме

- Подпись документа со стандартом CAdES
- Подпись документа со стандартом PAdES
- Добавление соподписи
- Установка личного сертификата
- Создание профиля подписи
- Переключение между профилями подписи
- Проверка подписи документа

Открыть статью на сайте

Шифрование

- О шифровании
- Шифрование документов
- Возможные ошибки

О шифровании

Шифрование — это процесс преобразования данных в форму, которая делает их недоступными для чтения без использования специальных средств, таких как ключ шифрования. Основная цель этой процедуры — обеспечить конфиденциальность информации, скрыв её от посторонних глаз, даже если у них есть доступ к зашифрованным данным.

Для шифрования файла вам понадобится открытый ключ получателя зашифрованных данных.

Как это работает?

- Вы выбираете сертификаты получателей или контакты с привязанными сертификатами.
- КриптоАРМ выполняет шифрование в адрес этих сертификатов.
- Получатели расшифровывают данные с помощью своего закрытого ключа.

> 💡 **Совет**: Для успешного шифрования убедитесь, что сертификаты получателей действительны и установлены в приложении.

Рекомендации

1. Добавление себя как получателя
    - Всегда добавляйте **свой личный сертификат** к списку получателей, если вы планируете в дальнейшем расшифровывать файл.
    - Если вы не добавите себя, то после шифрования не сможете открыть файл, даже если имели доступ к исходным данным.
2. Профили
    - При работе с несколькими получателями **используйте профиль шифрования**, чтобы сохранить настройки.
    - В профиле можно указать: включение архивации файлов, сохранение копий в «Архив», автоматическое добавление собственного сертификата как получателя.

3. Настройки безопасности
    - Убедитесь, что используемые алгоритмы шифрования соответствуют внутренним требованиям организации.
    - Если получатели используют разные криптопровайдеры, проверьте совместимость сертификатов перед шифрованием.

Шифрование документов

> 💡 **С чего начать**: Чтобы оценить, готово ли ваше рабочее место для шифрования документов, воспользуйтесь Проверкой рабочего места.

Шаг 1. Запуск мастера

1. Перейдите в раздел **Документы**.
2. Нажмите **Подпись и шифрование** в боковом меню раздела **Документы**.
3. Откроется новая вкладка с мастером.

> 💡 **Совет**: Открыть мастер можно с помощью действия **Добавить в** → **Подпись и шифрование** для файла в папке «Архив», результатах операции или в разделе «Почта».

Шаг 2. Добавление документов

Добавьте документы в мастер одним из способов:

1. Перетащите один или несколько файлов в окно приложения,
2. Загрузите с помощью кнопки **Загрузить с компьютера** или **Добавить из Архива**.

> 💡 **Совет**: Вы можете перетаскивать в мастер не только файлы, но и папки. При этом все файлы из вложенных папок также будут добавлены в мастер.

Шаг 3. Настройка параметров шифрования

> 💡 **Совет**: По умолчанию в мастере применяются настройки из активного профиля подписи. Вы можете переключаться между профилями, предварительно настроив в каждом нужные параметры для разных операций.

1. Выберите **Зашифровать** в блоке **Операции**.

Если необходимо создать зашифрованный архив, выберите **Архивировать**. В этом случае все файлы будут помещены в общий архив, который затем будет зашифрован.

2. Добавьте сертификаты получателей в блоке **Сертификаты шифрования**.
   - Нажмите на кнопку **Добавить сертификаты**.
   - В открывшемся окне выберите сертификат или контакт получателя. Для просмотра сведений о контакте и сертификате воспользуйтесь кнопкой .

> 💡 **Совет**: Чтобы иметь возможность расшифровать зашифрованный файл, добавьте личный сертификат к сертификатам шифрования.

3. Укажите настройки для сохранения результатов.
4. При необходимости укажите дополнительные настройки. Раскройте меню **Дополнительно**, чтобы изменить алгоритм, кодировку или формат файла.
5. Нажмите кнопку **Выполнить**.

Шаг 4. Подтверждение операции

Перед выполнением подписи запрашивается ее подтверждение.

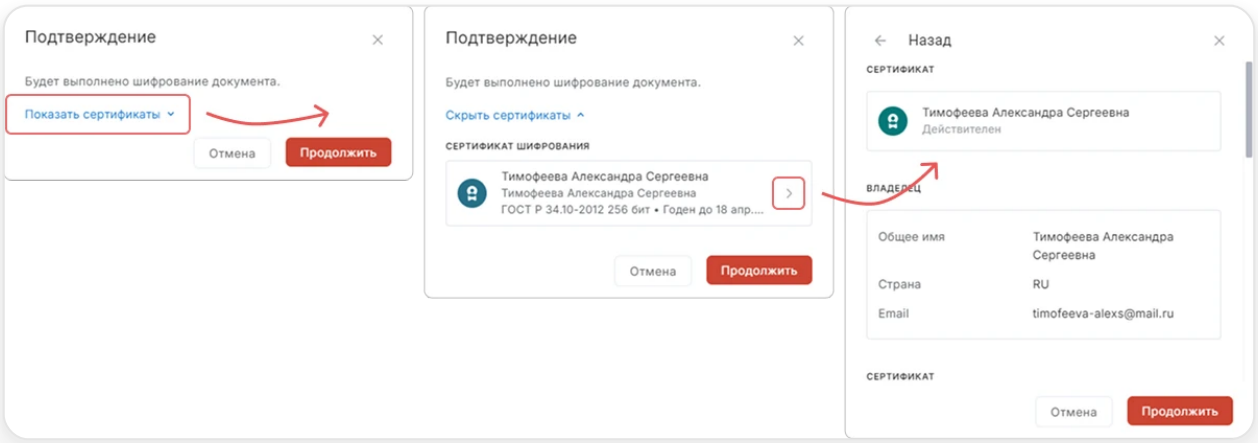
Чтобы подтвердить операцию:

1. Ознакомьтесь со сведениями в окне **Подтверждение**. Окно содержит сведения о количестве документов и выполняемой с ними операции, а также сертификатах, которые будут использоваться.
2. Нажмите кнопку **Продолжить**.

   Нажав «Продолжить» в окне, вы подтверждаете, что ознакомились с подписываемыми данными.

После подтверждения будет запущено выполнение операции.

> 💡 **Совет**: Чтобы просмотреть информацию о сертификате шифрования, нажмите на кнопку **Показать сертификат**. После этого нажмите на панель с сертификатом.

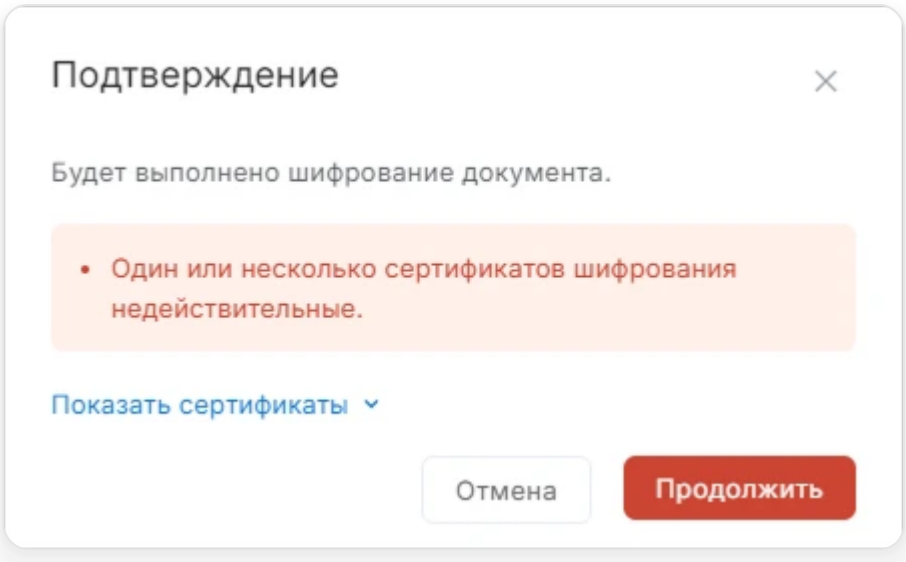


> 💡 **Совет**: Чтобы отменить операцию, нажмите на кнопку «Отмена». Следует помнить, что все операции с документами выполняются последовательно, и если вы нажмёте на кнопку, то операция будет остановлена на том документе, с которым производилась на момент отмены.

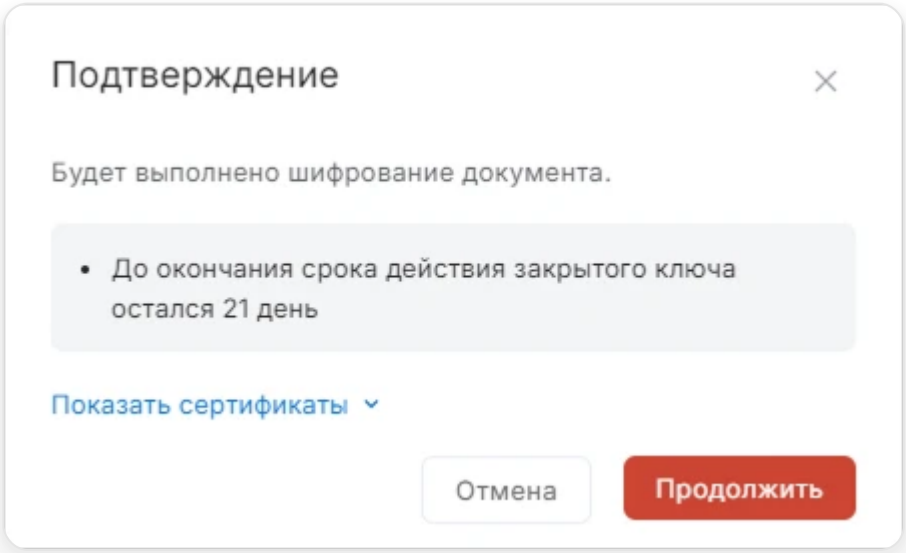
Дополнительные уведомления

В окне с подтверждением операции могут появиться дополнительные уведомления, если:

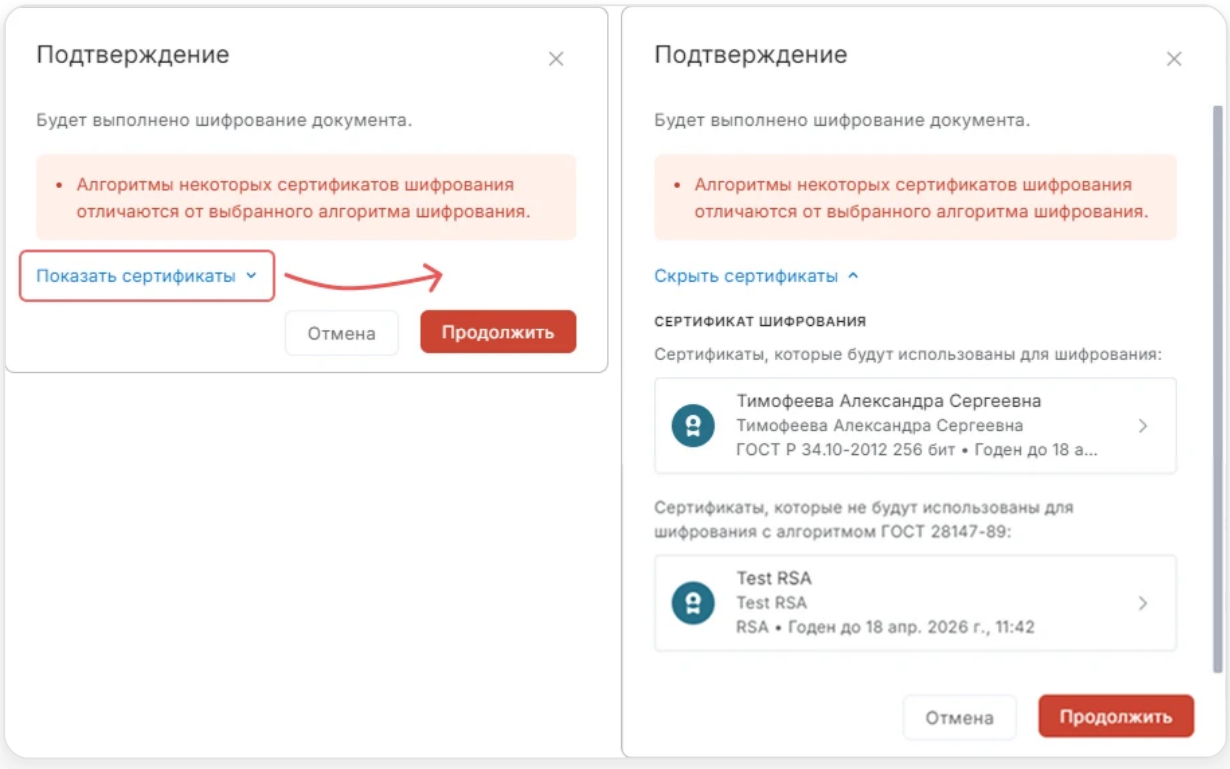
- Сертификат шифрования недействителен,



- Срок действия открытого или закрытого ключа личного сертификата 30 дней и менее,



- Алгоритмы сертификатов шифрования отличаются от выбранного алгоритма шифрования. В этом случае шифрование в адрес таких сертификатов не будет выполнено.



Шаг 5. Результат операции

Если операция прошла успешно, зашифрованные файлы будут сохранены в соответствии с указанными настройками.

> 💡 В окне с результатами операции вы можете отправить файл по электронной почте, сохранить его в «Архиве» и многое другое. Подробнее читайте в инструкции Действия с документами.

Возможные ошибки

При возникновении ошибки вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Рекомендуемые действия
Не удалось открыть файл	1. Проверьте наличие и доступность файлов 2. Убедитесь, что файлы не пустые (имеют ненулевой размер) 3. Повторите добавление файлов в мастер
Не удалось зашифровать файл	1. Проверьте права доступа к папке, указанной для сохранения результатов 2. Освободите место на диске
Отсутствует криптопровайдер для выбранного алгоритма шифрования	Установите криптопровайдер КриптоПро CSP и перезапустите приложение КриптоАРМ

Инструкции по теме

- Расшифрование документа
- Подпись документов со стандартом CAdES
- Подпись документов со стандартом PAdES
- Установка личного сертификата
- Создание профиля подписи
- Переключение между профилями подписи
- Проверка подписи документа
- Импорт сертификатов других пользователей
- Привязка сертификата к контакту

Открыть статью на сайте

Объединение подписей

- О функции
- Как объединить подписи

О функции

Функция **Объединение подписей** позволяет объединять несколько **отсоединенных подписей** в один файл подписи. Это удобно, когда:

- Необходимо создать **единый файл подписи** для документа, подписанного разными участниками;
- Требуется оптимизировать хранение подписей;
- Нужно подготовить файл для последующей проверки или архивации.

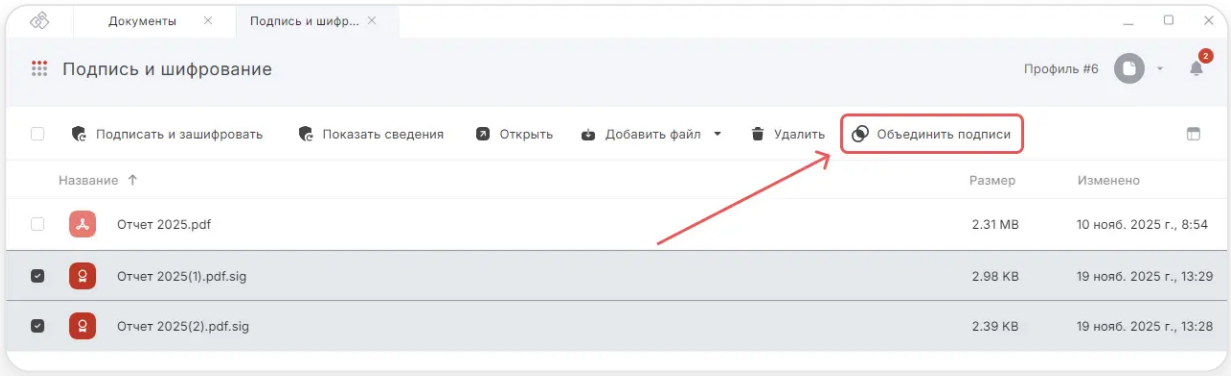
> 💡 **Примечание:** Объединенные подписи сохраняются отдельно и не изменяют исходные файлы.

Как объединить подписи

1. Перейдите в раздел **Документы**.
2. В боковом меню выберите **Подпись и шифрование**.
3. Откроется мастер работы с подписями в новой вкладке.

> 💡 **Совет:** Мастер можно открыть и через контекстное меню файла **Добавить в → Подпись и шифрование** (например, в папке «Архив», результатах операции или в разделе «Почта»).

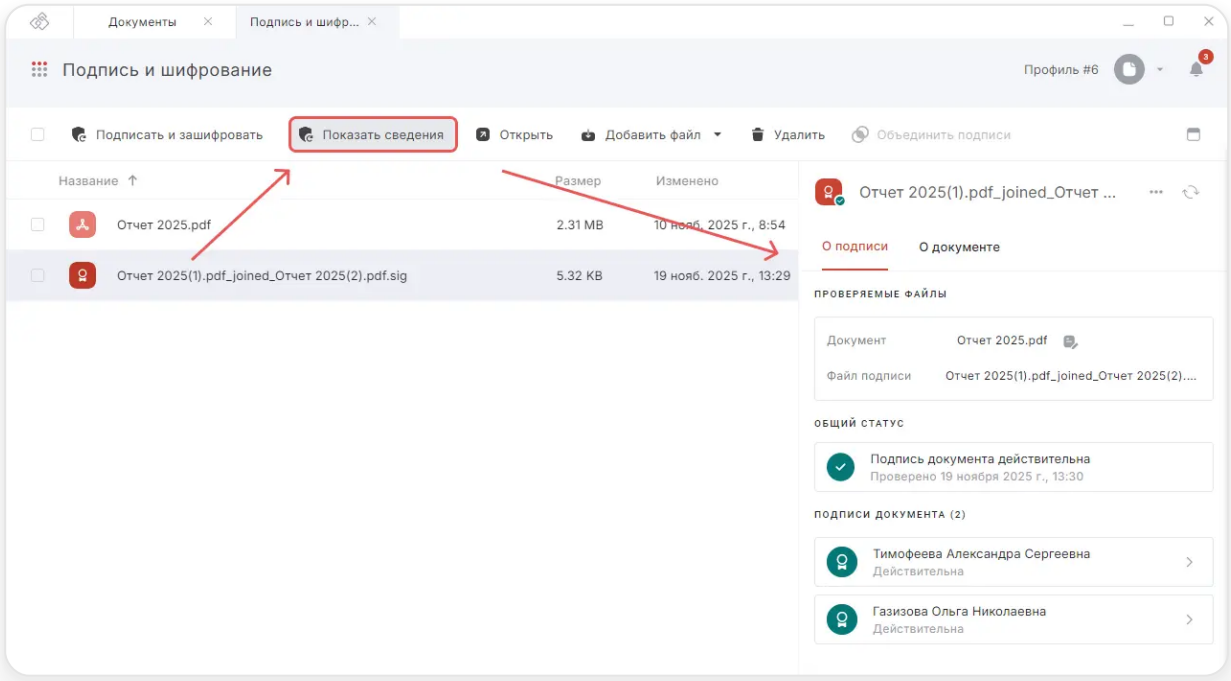
4. Добавьте файлы с отсоединенными подписями одним из способов:
    - **Перетащите** файлы в окно приложения;
    - Нажмите **Загрузить с компьютера**;
    - Или выберите **Добавить из Архива**.
5. Отметьте файлы для объединения с помощью **чекбоксов**.
6. Нажмите кнопку **Объединить подписи**.



> 💡 **Совет:** Выделять за раз можно не более двух файлов подписи.

- После нажатия выбранные подписи объединяются в **один новый файл**.
- Исходные файлы остаются без изменений, а новый файл получает суффикс `_joined` в названии.

7. Файл сохраняется в папку с исходными подписями.
   - Если исходные подписи находились в разных папках, файл сохраняется в **папке первого файла из списка**.
8. После завершения операции можно сразу проверить результат:
   - В списке файлов **выделите созданный объединённый файл** (с суффиксом `_joined`).
   - Нажмите **Показать сведения** на панели действий.



В открывшемся окне вы сможете увидеть общий статус подписи документа и список всех объединённых подписей.

> 💡 **Совет:** Если при проверке подписи появилось сообщение **Не удалось найти исходный файл для подписи**, укажите путь к исходному файлу документа. Это позволит приложению правильно связать подпись с исходным файлом и корректно отобразить сведения.

Полезные инструкции по теме

- Подпись документов со стандартом PAdES
- Добавление соподписи
- Установка личного сертификата
- Создание профиля подписи
- Переключение между профилями подписи
- Проверка подписи документа

Открыть статью на сайте

Проверка подписи

- Проверка подписи документа
- Проверка подписи документа с соподписями
- Распространенные проблемы
- Дополнительные действия
- Возможные ошибки

Проверка подписи документа

> 💡 **С чего начать**: Чтобы оценить, готово ли ваше рабочее место для работы с электронной подписью, воспользуйтесь Проверкой рабочего места.

Шаг 1. Запуск мастера

1. Перейдите в раздел **Документы**.
2. Нажмите **Проверка и расшифрование** в боковом меню раздела **Документы**.
3. Откроется новая вкладка с мастером.

Шаг 2. Добавление документов

Добавьте документы в мастер одним из способов:

1. Перетащите один или несколько файлов в окно приложения,
2. Загрузите с помощью кнопки **Загрузить с компьютера** или **Добавить из Архива**.

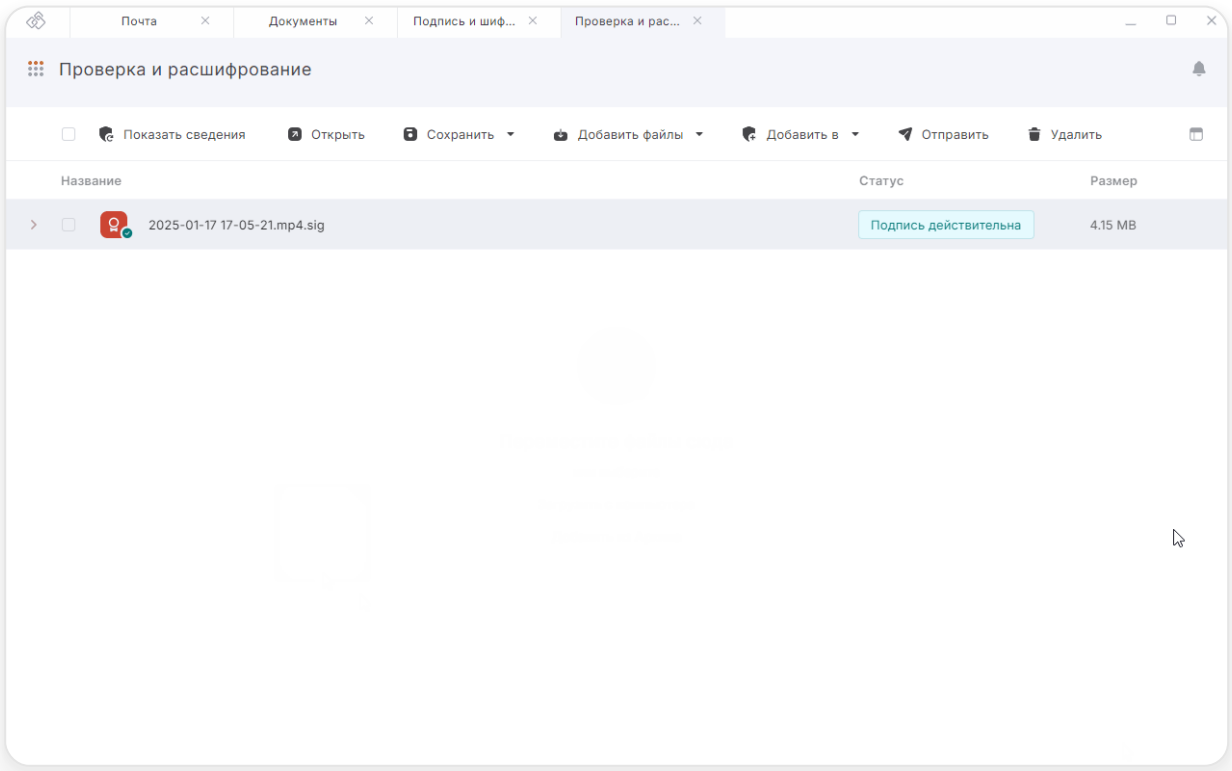
> 💡 **Совет**: Вы можете перетаскивать в мастер не только файлы, но и папки. При этом все файлы из вложенных папок также будут добавлены в мастер.
>
> 💡 **Совет**: В КриптоАРМ поддерживается проверка подписи для файлов с расширением `.sig`, `.p7s`, `.sgn`, `.sign`, `.bin` с ГОСТ и RSA/EC алгоритмами.

Шаг 3. Результаты проверки

Проверка запустится автоматически после добавления документов.

1. Статус подписи отобразится на панели с документом.

2. На иконке документа появится индикатор в виде:
   - зеленая галочка , если подпись действительная,
   - красный крестик, если недействительная.
3. Нажмите на кнопку **Показать сведения** .
4. В правой части окна отобразится область со сведениями о подписи.

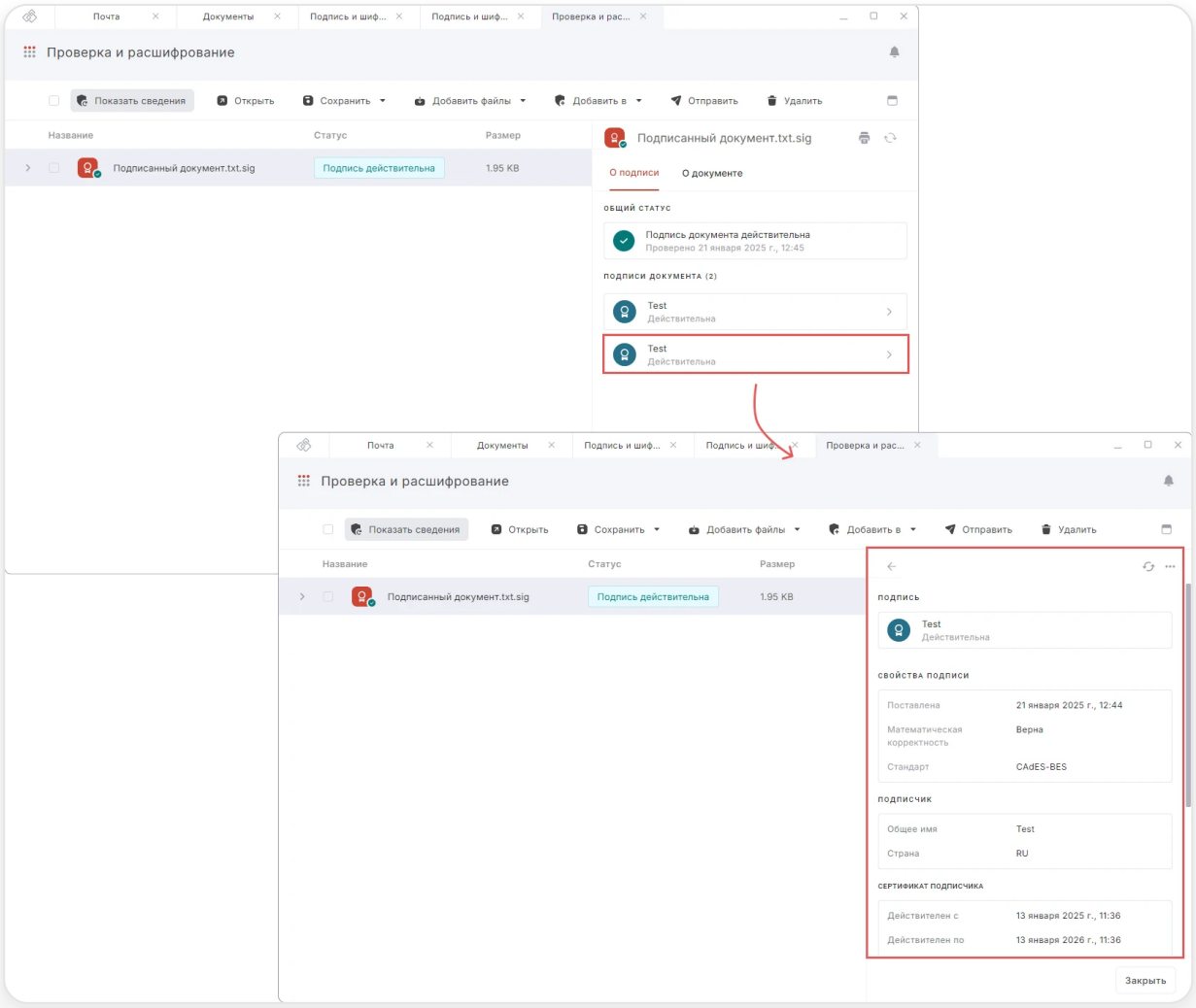


Статичный кадр демонстрации. Открыть анимацию

> 💡 **Совет**: Информация о подписи документа также доступна в мастере **Подпись и шифрование**, в папках **Архив** и **Почтовые вложения**. Подробнее в инструкции Просмотр информации о документе.

Проверка подписи документа с соподписями

1. Выполните шаги из инструкции Проверка подписи документа.
2. В блоке **Подписи документа** выберите подпись, сведения о которой необходимо просмотреть.
3. В области просмотра отобразятся сведения о подписи.



Распространенные проблемы

Почему подпись не проходит проверку или недействительна:

Причина	Возможность исправления	Рекомендуемые действия
Срок действия сертификата истёк или сертификат отозван	❌ Невозможно исправить	Запросите новый документ, подписанный действующим сертификатом
Документ изменён после подписания	❌ Невозможно исправить	Запросите оригинальную подписанную версию документа
Не построилась цепочка сертификации	✅ Можно исправить	Установите корневой и промежуточный сертификаты удостоверяющего центра, который выпустил ваш сертификат
	✅ Можно исправить	

Причина	Возможность исправления	Рекомендуемые действия
Неактуальный список отзыва (CRL)		Загрузите актуальный список отозванных сертификатов
Отсутствует криптопровайдер с поддержкой ГОСТ Р 34.10-2012	✅ Можно исправить	Установите криптопровайдер КриптоПро CSP и перезапустите приложение КриптоАРМ

Дополнительные действия

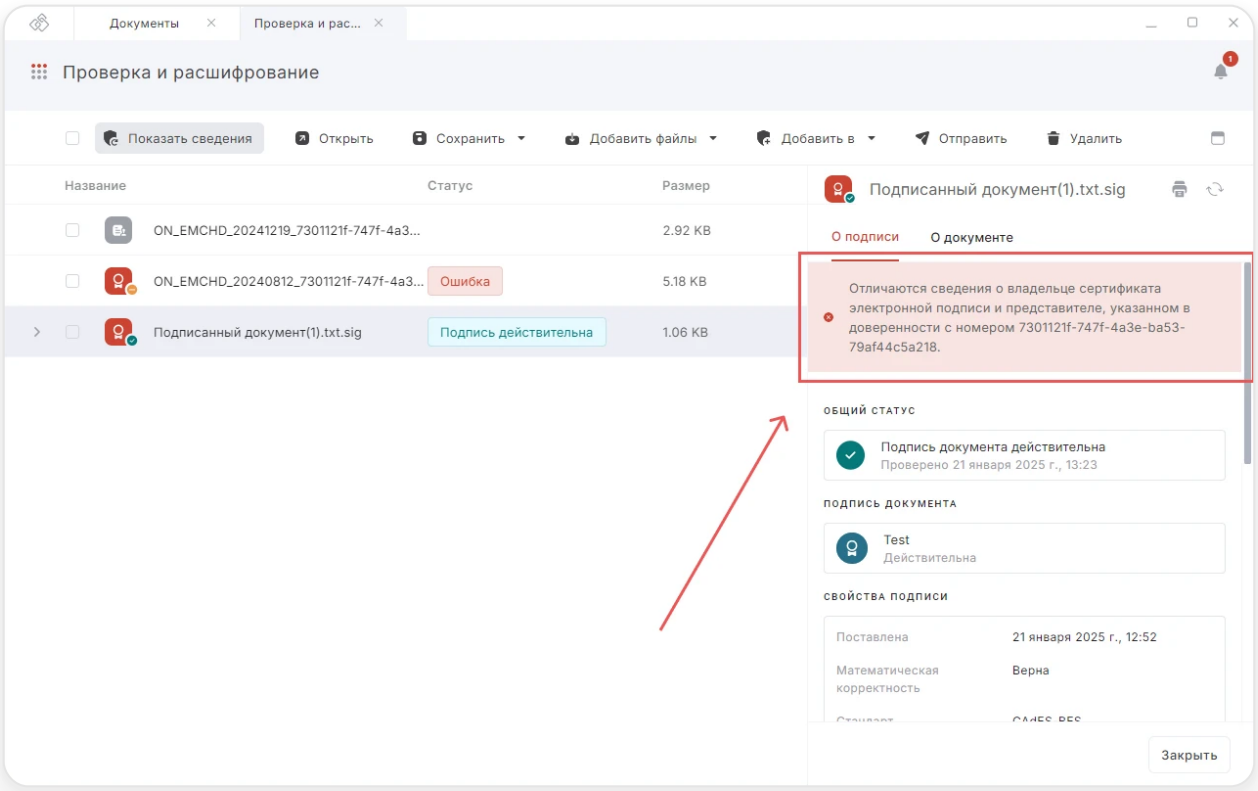
Проверка соответствия МЧД сертификату подписи

При проверке подписи производится дополнительная проверка данных владельца сертификата подписи и владельца машиночитаемой доверенности. Эта проверка осуществляется на основании реквизита ИНН.

> ⚠️ **Примечание**: Проверка доступна для документов, содержащих одну подпись.

Чтобы выполнить проверку:

1. Добавьте в мастер подписанные документы и машиночитаемую доверенность с файлом подписи.
2. Нажмите на кнопку **Показать сведения** 
3. В правой части окна отобразится область со сведениями о подписи. Если проверка не пройдет успешно, отобразится уведомление: «Сведения о владельце сертификата подписи отличаются от данных в машиночитаемой доверенности».



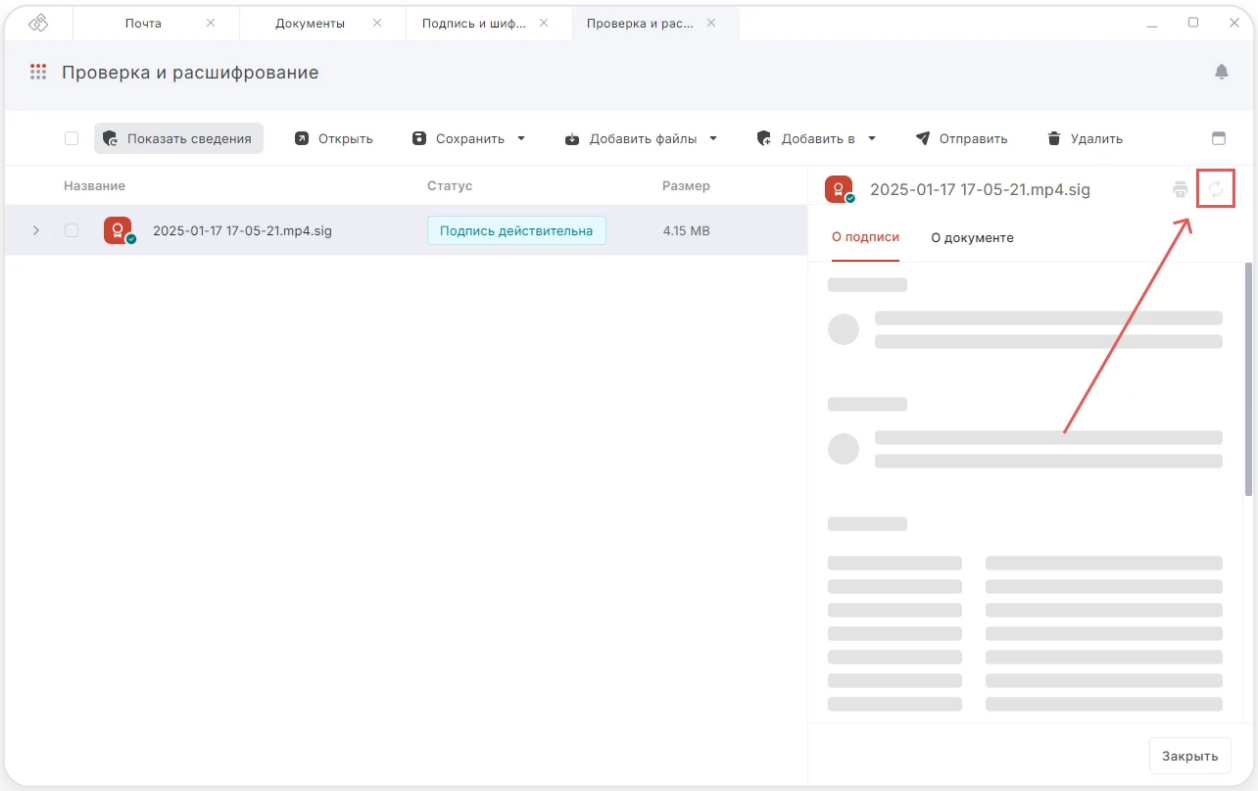
Обновление сведений о подписи

В некоторых случаях, например, при установке корневого или промежуточного сертификата, может потребоваться повторная проверка подписи документа.

Чтобы обновить сведения о подписи документа:

1. Выполните шаги из инструкции Проверка подписи документа.
2. В области просмотра со сведениями о подписи нажмите на кнопку **Обновить** .

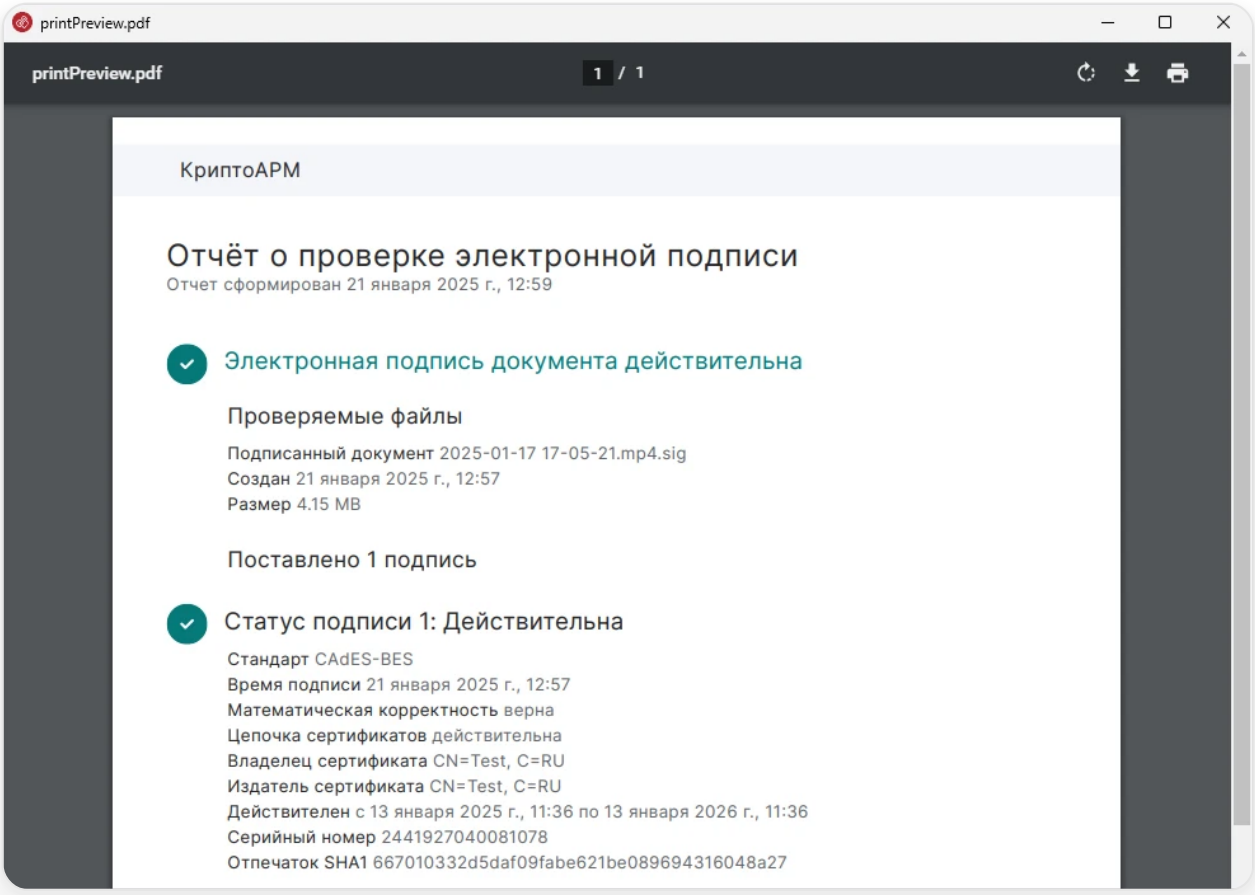
Сведения о подписи будут обновлены.



Печать сведений о подписи

1. Выполните шаги из инструкции Проверка подписи документа.
2. Нажмите на кнопку **Печать** .
3. Откроется окно с отчетом о проверке электронной подписи.

Отчет можно распечатать или скачать на устройство.



Возможные ошибки

При возникновении ошибки вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Рекомендуемые действия
Не удалось открыть файл	1. Проверьте наличие и доступность файла 2. Повторите добавление файла в мастер
Не удалось найти исходный файл для подписи	Добавьте в мастер исходный файл, для которого была сделана отсоединенная подпись, либо укажите путь к файлу в области справа.

Инструкции по теме

- Подпись документа со стандартом CAdES
- Подпись документа со стандартом PAdES
- Установка личного сертификата

- Создание профиля подписи
- Переключение между профилями подписи
- Импорт сертификатов других пользователей
- Привязка сертификата к контакту

Открыть статью на сайте

Снятие подписи

- Снятие подписи с документа
- Возможные ошибки

Снятие подписи с документа

> 💡 **С чего начать**: Чтобы оценить, готово ли ваше рабочее место для работы с электронной подписью, воспользуйтесь Проверкой рабочего места.

Шаг 1. Запуск мастера

1. Перейдите в раздел **Документы**.
2. Нажмите **Проверка и расшифрование** в боковом меню раздела **Документы**.
3. Откроется новая вкладка с мастером.

Шаг 2. Добавление документов

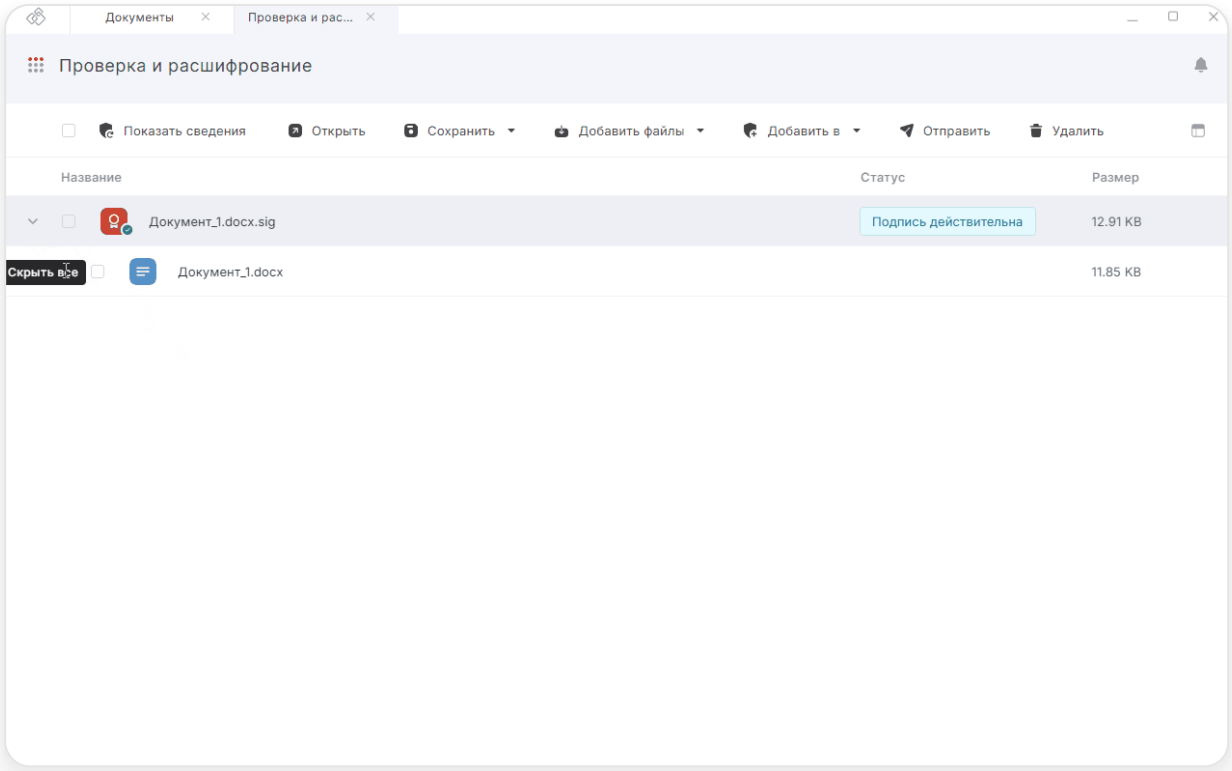
Добавьте документы в мастер одним из способов:

1. Перетащите один или несколько файлов в окно приложения,
2. Загрузите с помощью кнопки **Загрузить с компьютера** или **Добавить из Архива**.

> 💡 **Совет**: Вы можете перетаскивать в мастер не только файлы, но и папки. При этом все файлы из вложенных папок также будут добавлены в мастер.

Шаг 3. Результаты

1. После добавления документов запустится автоматическое расшифрование и проверка подписи.
2. Нажмите кнопку › слева от файла, с которого нужно снять подпись.
3. В списке отобразится исходный документ без подписи.
4. Выполните необходимое действие с документом.



Статичный кадр демонстрации. Открыть анимацию

Возможные ошибки

При возникновении ошибки вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Рекомендуемые действия
Не удалось открыть файл	1. Проверьте наличие и доступность файла 2. Повторите добавление файла в мастер
Нельзя снять открепённую подпись с файла	При открепленной подписи оригинал документа и так находится в отдельном файле

Инструкции по теме

- Подпись документа со стандартом CAdES
- Подпись документа со стандартом PAdES
- Установка личного сертификата
- Создание профиля подписи
- Переключение между профилями подписи
- Импорт сертификатов других пользователей

- Привязка сертификата к контакту

Открыть статью на сайте

Расшифрование

- Перед началом работы
- Расшифрование документа
- Возможные ошибки

Перед началом работы

Прежде чем приступить к расшифрованию документа, убедитесь, что рабочее место готово, а все необходимые инструменты установлены.

1. **Проверьте лицензии**: убедитесь в наличии действующих лицензий на КриптоАРМ и КриптоПро CSP. Без действующих лицензий расшифровать документ невозможно. Подробнее про лицензии читайте в инструкции Лицензирование.
2. **Установите личный сертификат**: в хранилище **Личные сертификаты** должен быть установлен сертификат, в адрес которого было выполнено шифрование. Подробная инструкция: Установка личного сертификата.

> 💡 **С чего начать**: Чтобы оценить, готово ли ваше рабочее место для расшифрования документов, воспользуйтесь Проверкой рабочего места.

Расшифрование документа

Шаг 1. Запуск мастера

1. Перейдите в раздел **Документы**.
2. Нажмите **Проверка и расшифрование** в боковом меню раздела **Документы**.
3. Откроется новая вкладка с мастером.

Шаг 2. Добавление документов

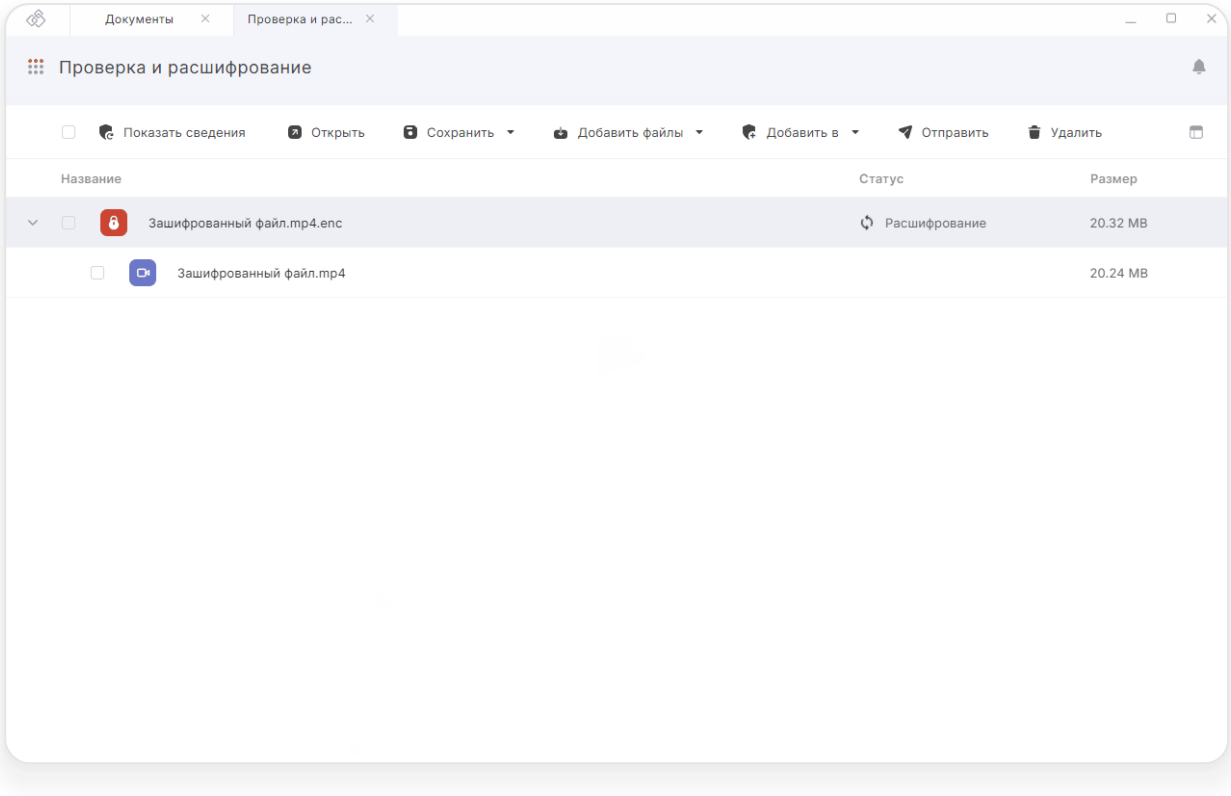
Добавьте документы в мастер одним из способов:

1. Перетащите один или несколько файлов в окно приложения,
2. Загрузите с помощью кнопки **Загрузить с компьютера** или **Добавить из Архива**.

> 💡 **Совет**: Вы можете перетаскивать в мастер не только файлы, но и папки. При этом все файлы из вложенных папок также будут добавлены в мастер.

Шаг 3. Результаты операции

1. После добавления документов запустится автоматическое расшифрование и проверка подписи (если есть).
2. При необходимости укажите пароль на контейнер с личным сертификатом.
3. Расшифрованный фаил отобразится под зашифрованным. На панели с зашифрованным документом отобразится статус «Расшифрован».



Статичный кадр демонстрации. Открыть анимацию

Шаг 4. Сохранение результатов

При успешном расшифровании полученные оригиналы документов сохраняются во временной папке и удаляются автоматически после закрытия приложения.

Чтобы сохранить расшифрованные файлы:

1. Выделите в списке файлы, которые нужно сохранить.
2. Выберите одно из действий:
   - **Сохранить** - для сохранения на компьютере или в **Архиве**,
   - **Отправить** - для отправки в качестве вложения в письме.

Возможные ошибки

При возникновении ошибки вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Рекомендуемые действия
Не удалось открыть файл	1. Проверьте наличие и доступность файла 2. Повторите добавление файла в мастер
Не удалось расшифровать файл	1. Убедитесь, что файл не пустой (имеет ненулевой размер). 2. Убедитесь в наличии сертификата для расшифрования.
Не удалось расшифровать файл	Установите криптопровайдер КриптоПро CSP и перезапустите приложение КриптоАРМ
Отсутствует действующая лицензия КриптоАРМ	1. Приобретите или продлите лицензию КриптоАРМ 2. Активируйте лицензию в настройках программы
Отсутствует действующая лицензия КриптоПро CSP	Установите лицензию КриптоПро CSP

Инструкции по теме

- Шифрование документа
- Установка личного сертификата
- Создание профиля подписи
- Переключение между профилями подписи
- Проверка подписи документа
- Импорт сертификатов других пользователей
- Привязка сертификата к контакту

Открыть статью на сайте

Просмотр документа

- Открытие документа
- Инструменты просмотра
- Возможные ошибки

Открытие документа

Шаг 1. Запуск мастера

1. Перейдите в раздел **Документы**.
2. Нажмите **Подпись и защита PDF** в боковом меню раздела **Документы**.
3. Откроется новая вкладка с мастером.

> 💡 **Совет**: Открыть мастер можно с помощью действия **Добавить в** → **Подпись и защита PDF** для файла в папке «Архив», результатах операции или в разделе «Почта».

Шаг 2. Добавление документа

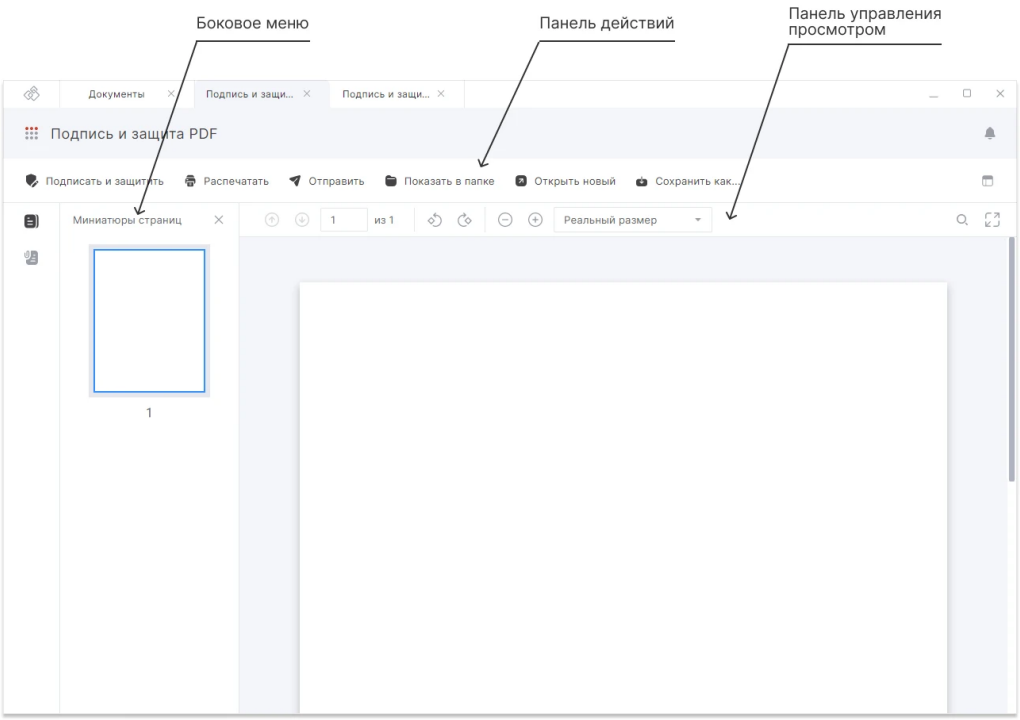
Добавьте документ в мастер одним из способов:

1. Перетащите в окно приложения,
2. Загрузите с помощью кнопки **Загрузить с компьютера**.

После загрузки документ будет открыт для просмотра.

Если в документе есть подписи, то КриптоАРМ автоматически запустит их проверку. Подробнее про проверку подписи читайте в инструкции.

Инструменты просмотра



Панель действий

Кнопка	Функция	Иконка
Подписать и защитить	Переход к настройкам подписи и разметке областей	-
Распечатать	Печать документа	-
Показать в папке	Открытие расположения файла	-
Открыть новый	Замена текущего документа	-
Сохранить как	Создание копии файла	-
Подробно	Открытие панели сведений	

Панель управления просмотром

Элемент	Функция	Иконка
Навигация по страницам		

Элемент	Функция	Иконка
	Листание и переход к конкретной странице	
Поворот страниц	Вращение на 90°	
Масштабирование	Увеличение/уменьшение просмотра	
Поиск по тексту	Нахождение слов в документе	-
Режим просмотра	Полноэкранный/обычный режим	

> ⚠️ **Важно**: Поворот страниц не изменяет исходный файл - только режим просмотра

Боковое меню навигации

- **Миниатюры страниц** – отображение панели с миниатюрным представлением страниц. При выборе миниатюры страницы происходит переход к нужной странице документа в основной области.
- **Вложения** – открытие панели вложений со списком вложенных файлов. Вложенные файлы могут быть открыты для просмотра средствами ОС.
- **Подписи** – отображение панели с проставленными подписями и свободными областями для подписантов.

Возможные ошибки

При возникновении ошибки вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Описание	Рекомендуемые действия
Не удалось открыть файл	Файл поврежден или не является PDF	Попробуйте открыть файл в другом приложении или запросите оригинал документа у отправителя
Не удалось открыть файл	Установлены ограничения на просмотр. Возможно, документ защищен паролем.	1. Запросите у отправителя пароль для снятия защиты 2. Попросите предоставить незащищенную версию
Файл не соответствует формату PDF	Выбран файл, несоответствующий формату PDF	

Ошибка	Описание	Рекомендуемые действия
		Убедитесь, что расширение файла соответствует формату PDF и попробуйте добавить файл еще раз

Инструкции по теме

- Подпись PDF-документа
- Проверка подписи PDF-документа
- Установка личного сертификата
- Создание профиля подписи
- Переключение между профилями подписи

Открыть статью на сайте

Подпись документа

- Подпись документа PDF
- Действия в мастере
- Возможные ошибки

В мастере **Подпись и защита PDF** КриптоАРМ поддерживает создание встроенной электронной подписи по стандарту PAdES. Подробнее о подписи можно прочитать в инструкции О подписи PAdES.

Подпись документа PDF

> 💡 **С чего начать**: Чтобы оценить, готово ли ваше рабочее место для работы с электронной подписью, воспользуйтесь Проверкой рабочего места.

Шаг 1. Запуск мастера

1. Перейдите в раздел **Документы**.
2. Нажмите **Подпись и защита PDF** в боковом меню раздела **Документы**.
3. Откроется новая вкладка с мастером.

> 💡 **Совет**: Открыть мастер можно с помощью действия **Добавить в** → **Подпись и защита PDF** для файла в папке «Архив», результатах операции или в разделе «Почта».

Шаг 2. Добавление документа

Добавьте документ в мастер одним из способов:

1. Перетащите в окно приложения,
2. Загрузите с помощью кнопки **Загрузить с компьютера**.

После загрузки документ будет открыт для просмотра.

Шаг 3. Настройки подписи

> 💡 **Совет**: По умолчанию в мастере применяются настройки из активного профиля подписи. Вы можете переключаться между профилями, предварительно настроив в каждом нужные параметры для разных операций.

1. Нажмите на кнопку **Подписать и защитить** на панели действий.
2. В правой части окна отобразятся настройки подписи.
3. В блоке **Настройте свою подпись** выберите:
   - Личный сертификат,
   - Стандарт подписи,
   - Разместите штамп для личной подписи и настройте его оформление, если необходимо поставить «видимую» подпись.
4. При необходимости установите дополнительные настройки:
   - Добавьте подписантов,
   - Добавьте произвольную область и настройте ее оформление,
   - Добавьте сертификацию,
   - Добавьте конвертацию.
5. Укажите настройки для сохранения результата операции.
6. Нажмите кнопку **Выполнить**.

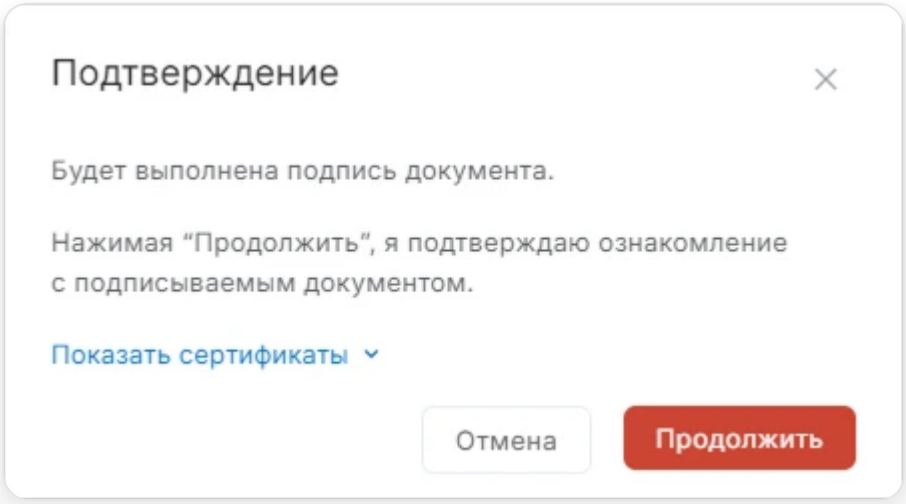
Шаг 4. Подтверждение операции

Перед выполнением подписи запрашивается ее подтверждение.

Чтобы подтвердить операцию:

1. Ознакомьтесь со сведениями в окне **Подтверждение**.
2. Нажмите кнопку **Продолжить**.

   Нажав «Продолжить» в окне, вы подтверждаете, что ознакомились с подписываемыми данными.



После подтверждения будет запущено выполнение операции.

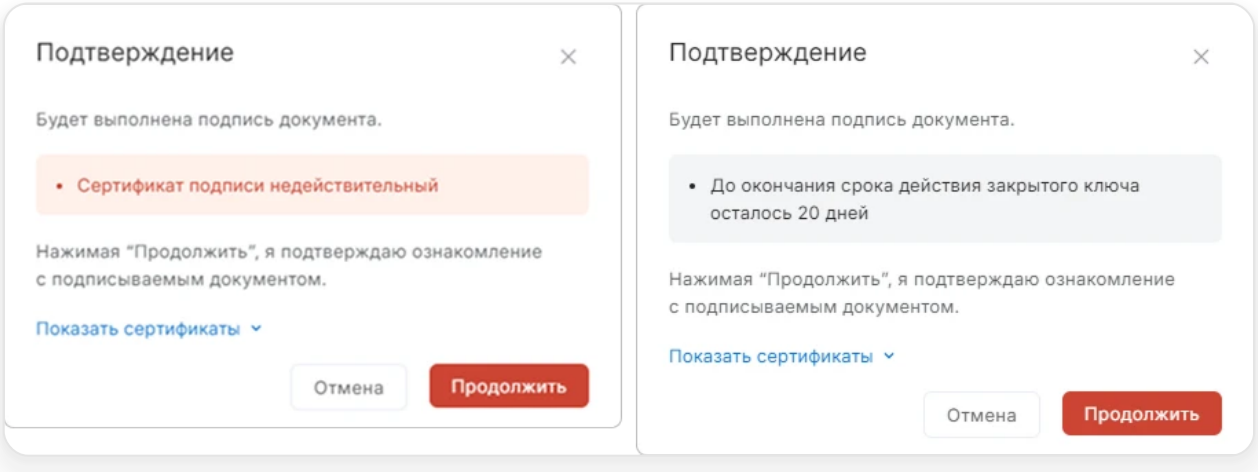
> 💡 **Совет**: Чтобы просмотреть информацию о сертификате подписи, нажмите на кнопку **Показать сертификат**. После этого нажмите на панель с сертификатом.

Дополнительные уведомления

В окне с подтверждением операции могут появиться дополнительные уведомления, если:

- Сертификат подписи недействителен,
- Срок действия открытого или закрытого ключа личного сертификата 30 дней и менее,

> 🚨 **Важно**: Во перечисленных случаях подпись будет выполнена, но стоит учесть, что её действительность может быть поставлена под сомнение.



Шаг 5. Результат операции

Если операция прошла успешно, подписанный файл будет сохранен в соответствии с указанными настройками.

Подписанный документ открывается в режиме просмотра и проверки подписи.

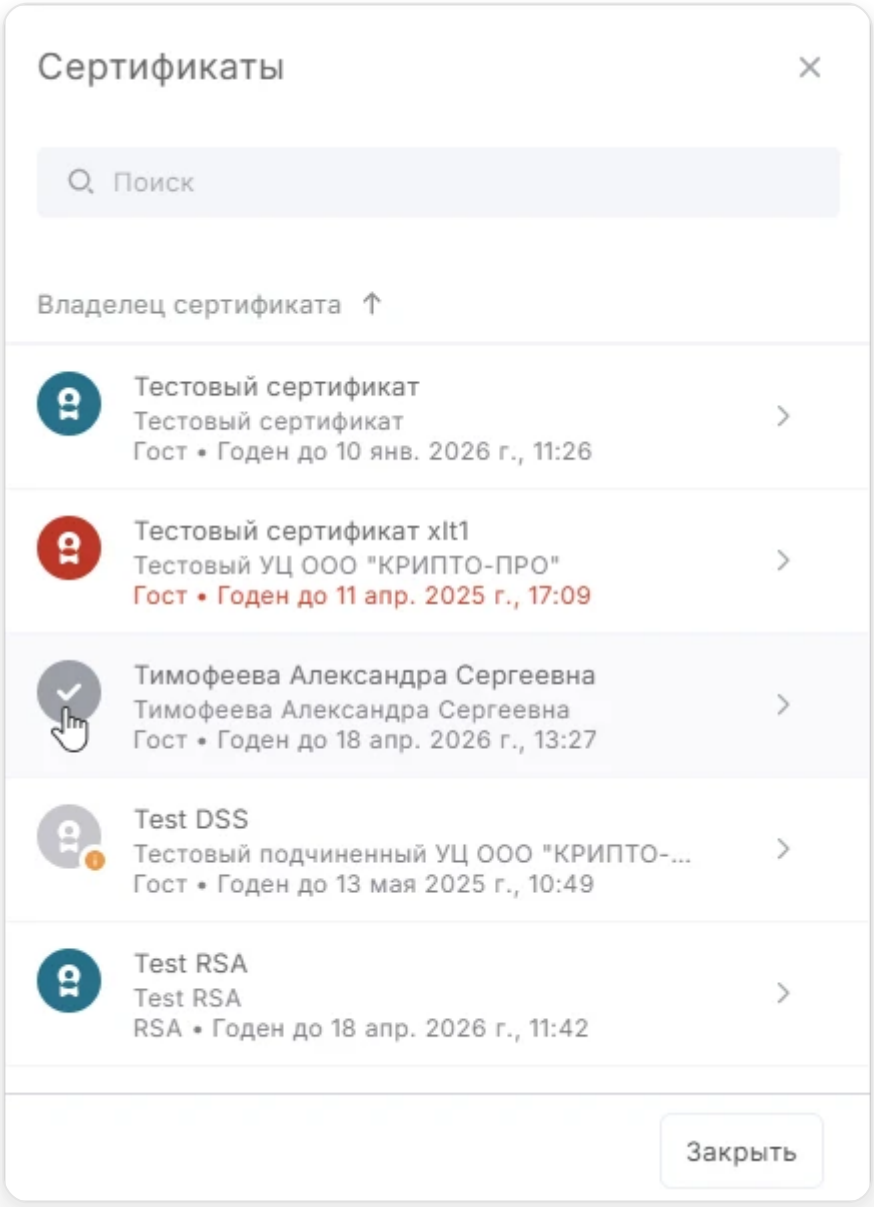
> 💡 В окне с результатами операции вы можете ознакомиться с информацией о подписи, распечатать файл или отправить его по электронной почте или сохранить его в «Архиве».

Действия в мастере

1. Выбор сертификата в мастере

Чтобы выбрать сертификат:

1. Нажмите на кнопку **Редактировать**  в блоке **Настройте свою подпись**.
2. В открывшейся правой боковой панели отметьте чекбоксом нужный сертификат.

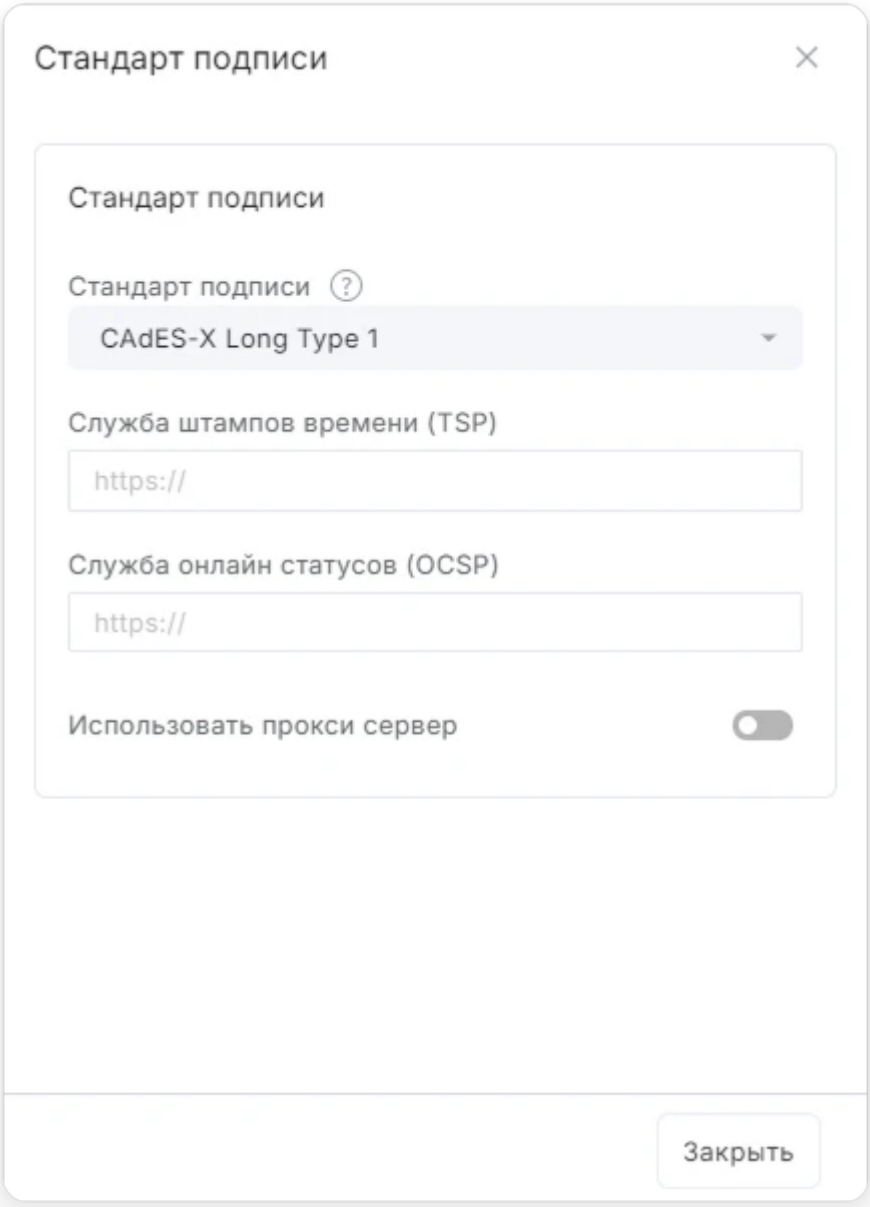


3. Закройте панель с помощью кнопки **Закрыть**.

2. Настройка стандарта подписи в мастере

Чтобы выбрать стандарт подписи:

1. Нажмите кнопку **Редактировать** в блоке **Стандарт подписи**.
2. В появившейся правой боковой панели выставите необходимый стандарт подписи.



Для стандартов со штампами потребуется указать дополнительные настройки служб штампов времени. Подробнее читайте в инструкции Настройки для стандартов со штампами.

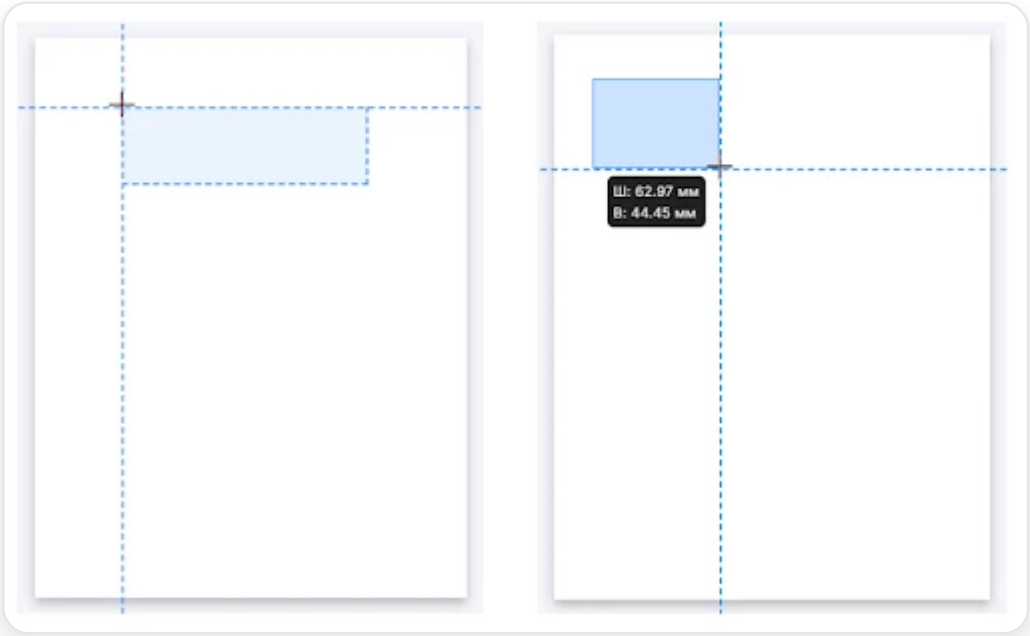
3. Закройте панель с настройкой стандарта подписи по кнопке **Закрыть**.

3. Разметка области для штампа подписи

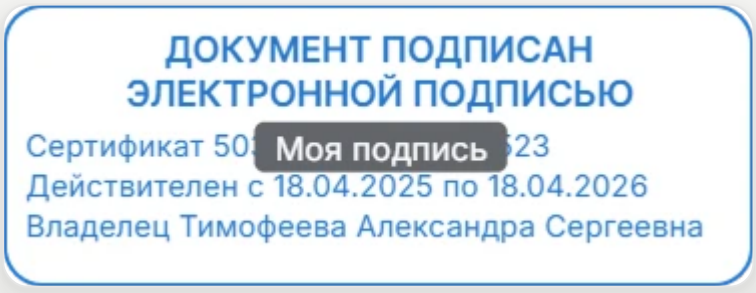
Чтобы разместить штамп для видимой подписи:

1. Нажмите кнопку **Разметить** в блоке **Визуализация**.
2. На странице документа появятся пунктирные направляющие. При наведении курсора мыши на пересечении направляющих отобразится схематичный прямоугольник.

3. Наведите курсор мыши в место размещения штампа на странице документа и кликните левой кнопкой мыши. В этом случае размер области будет соответствовать размеру схематичного прямоугольника. Для того чтобы задать собственный размер области, наведите курсор мыши в место размещения штампа и, зажав левую кнопку мыши, разметьте область нужного размера.

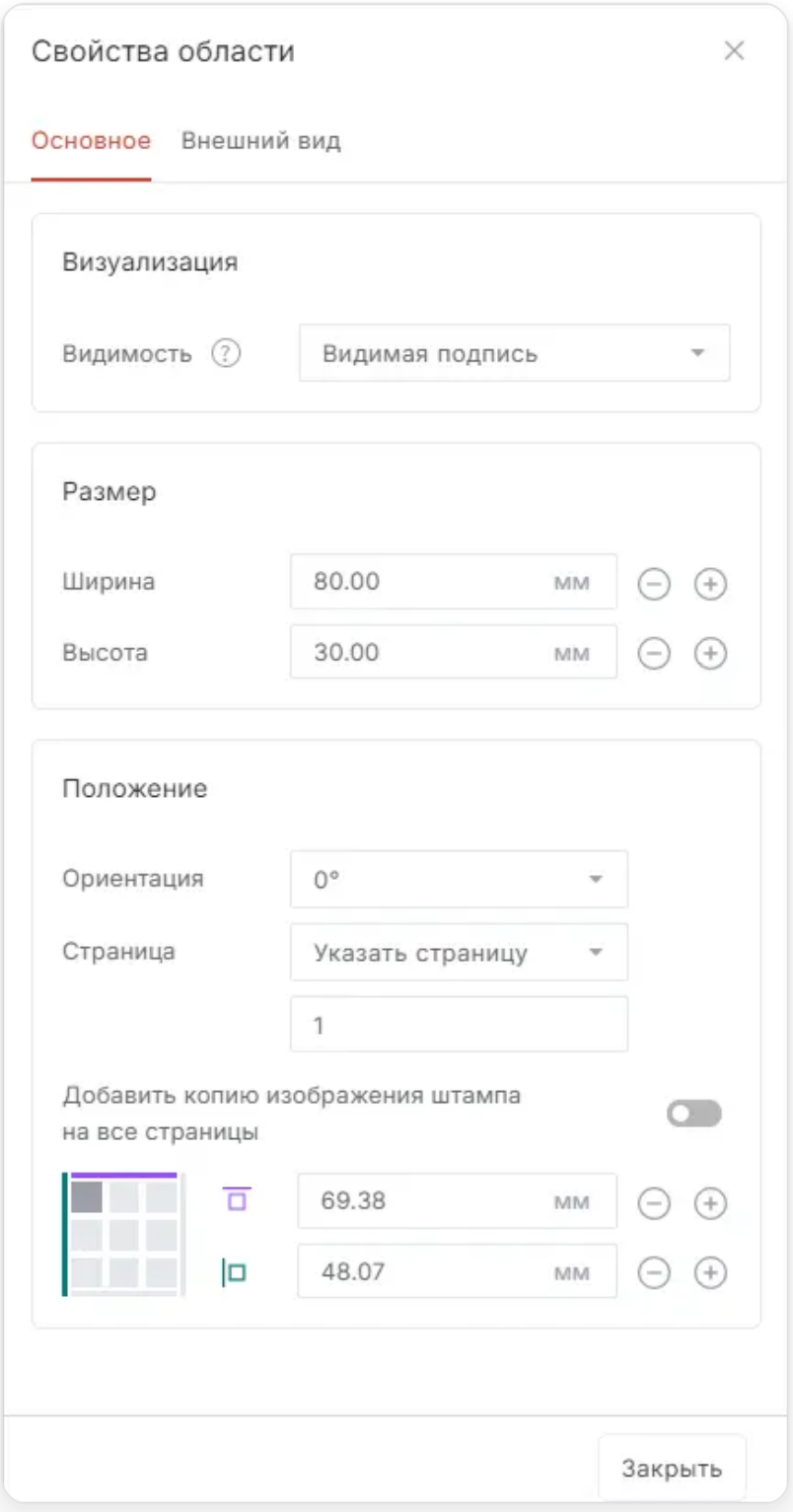


⚠️ **Примечание**: После разметки в области появится лейбл **Моя подпись**. Данный лейбл служит исключительно для визуального ориентира и исчезнет после подписи документа.



4. Изменение размера и положения области для штампа подписи

1. Нажмите на кнопку **Свойства** на панели **Визуализация**.
2. Откроется окно **Свойства области**.



3. Внесите необходимые изменения и закройте окно.

5. Изменение вида подписи с видимой на невидимую

1. Нажмите на кнопку **Свойства** на панели **Визуализация**.
2. Откроется окно **Свойства области**.

3. В разделе **Визуализация** установите для параметра **Видимость** значение **Невидимая подпись**.
4. Закройте окно по кнопке **Закрыть**.

6. Настройка оформления штампа подписи

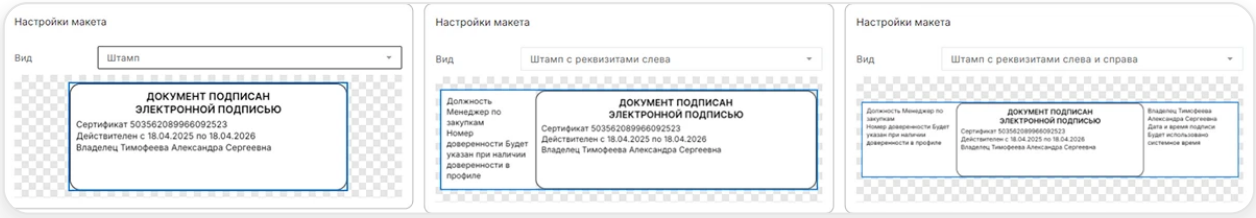
> 💡 По умолчанию визуализация информации об электронной подписи задается в соответствии с требованиями ГОСТ Р 7.0.97-2016. В штамп подписи выводятся заголовок «Документ подписан электронной подписью», серийный номер сертификата, имя владельца сертификата и срок действия сертификата.

1. Разместите область для штампа подписи.
2. Нажмите на кнопку **Свойства** на панели **Визуализация**.
3. В появившемся окне перейдите на вкладку **Внешний вид**.

1. Вид штампа

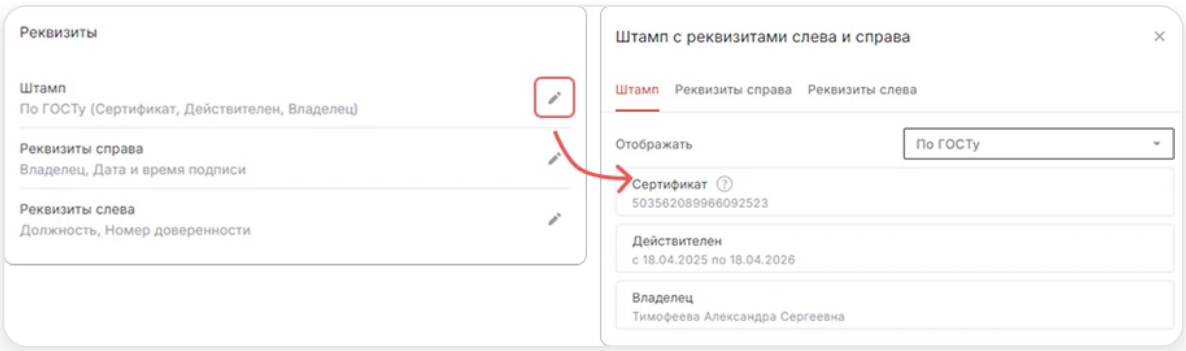
Выберите макет штампа в настройке **Вид**:

- **Штамп** - в области будет размещен только штамп.
- **Штамп с реквизитами слева** - в области будет размещен штамп, а также блок с реквизитами слева от штампа.
- **Штамп с реквизитами справа** - в области будет размещен штамп, а также блок с реквизитами справа от штампа.
- **Штамп с реквизитами слева и справа** - в области будет размещен штамп, а также блок с реквизитами слева и справа от штампа.

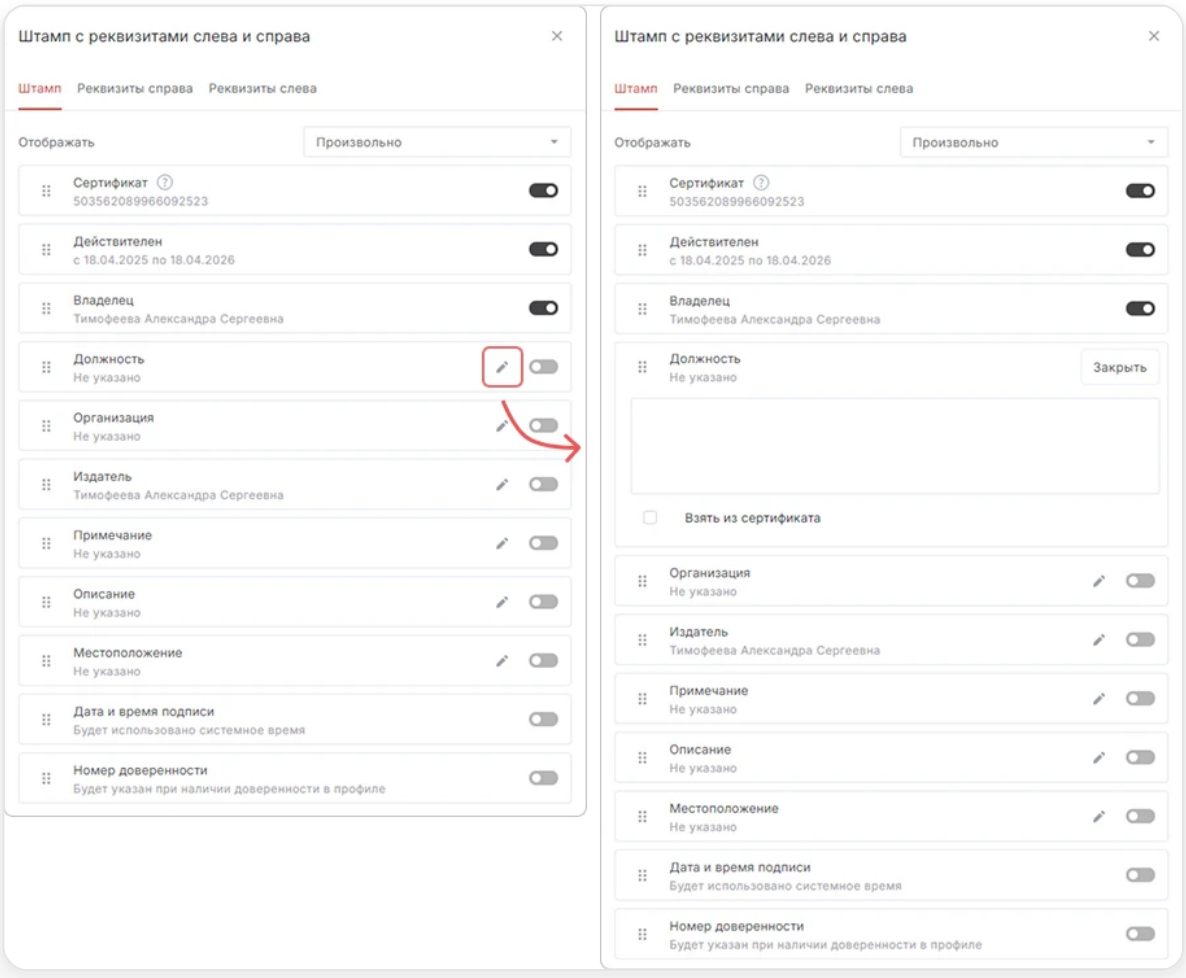


2. Настройка реквизитов

1. Нажмите на кнопку **Редактировать** в блоке **Реквизиты**.
2. В открывшемся окне укажите настройки отображения:
    - **По ГОСТу** - для вывода реквизитов в соответствии с **ГОСТ Р 7.0.97-2016**.



- **Произвольно** - для самостоятельной настройки реквизитов.
  - Активируйте переключатели нужных реквизитов.
  - При необходимости измените порядок отображения реквизитов с помощью кнопки ⠿. Наведите курсор мыши на кнопку и, удерживая левую кнопку мыши на кнопке, переместите реквизит в необходимое место в списке.
  - При необходимости настройте значения реквизитов. По умолчанию они берутся из сертификата подписи. Чтобы указать свои значения, нажмите на кнопку **Редактировать**, расположенную на панели с реквизитом. Снимите флажок **Взять из сертификата** и введите новое значение в соответствующее поле.



3. Аналогичным образом настройте вывод реквизитов для блоков слева или справа от штампа, если их отображение активировано.

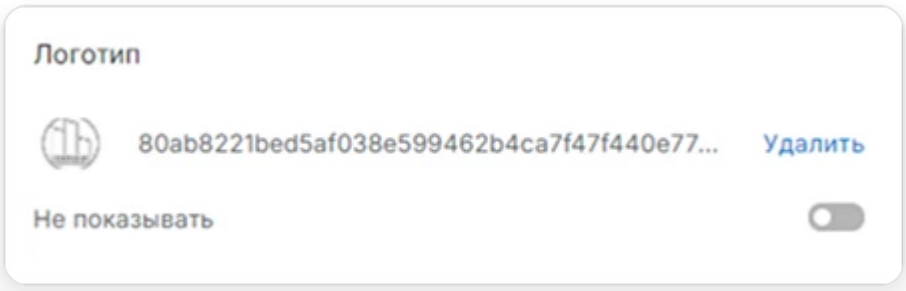
> 💡 **Примечание:** По умолчанию в поле **Владелец** штампа отображается значение **Общее имя (CN)** из сертификата. Если в сертификате указано название организации, а требуется вывести ФИО подписанта, откройте **Настройки визуализации** → **Внешний вид** → **Редактировать** в блоке «Реквизиты», выберите тип штампа «Произвольно» и включите переключатель «ФИО».

3. Оформление

1. Активируйте переключатель **Добавить фон на область** для добавления фона с цветом: #ffffff (hex).
2. Активируйте переключатель **Добавить границу на оттиск подписи** для добавления границы.
3. Настройте цвет границы и текста одним из способов:
   - Выберите необходимый цвет в палитре,
   - Укажите код цвета в hex-формате



4. Загрузите изображение с гербом или эмблемой в блоке **Логотип**.
   - Нажмите на кнопку **Загрузить**,
   - Укажите путь к файлу в окне файлового менеджера.

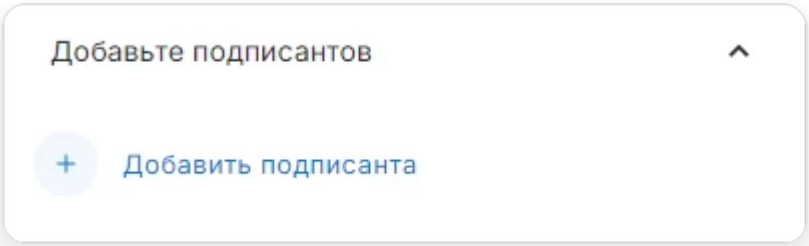


7. Подписанты

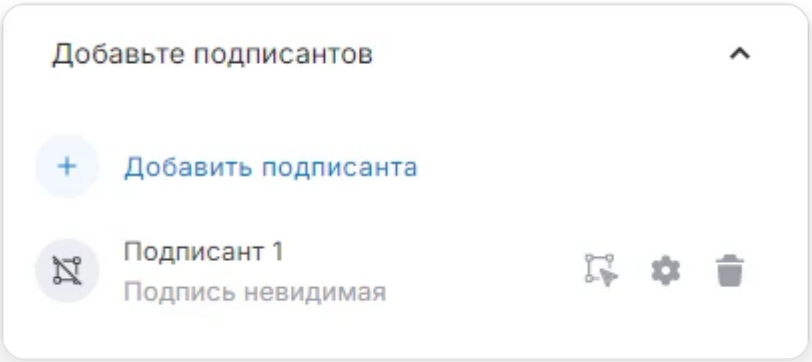
Добавление подписантов

> 💡 В приложении в документ можно добавить до 10 подписантов. По аналогии с личной подписью подпись подписантов может быть видимой и невидимой.

1. Нажмите кнопку **Добавить подписанта**.



2. В блоке **Добавьте подписантов** появится подписант с невидимой подписью.



Разметка области для подписи подписанта

1. Нажмите кнопку **Разметить** на панели с подписантом.
2. На странице документа появятся пунктирные направляющие. При наведении курсора мыши на пересечении направляющих отобразится схематичный прямоугольник.
3. Наведите курсор мыши в место размещения штампа на странице документа и кликните левой кнопкой мыши. В этом случае размер области будет соответствовать размеру схематичного прямоугольника. Для того, чтобы задать собственный размер области, наведите курсор мыши в место размещения штампа и, зажав левую кнопку мыши, разметьте область нужного размера.

> ⚠️ **Примечание**: После разметки в области появится лейбл с названием подписанта. Данный лейбл служит исключительно для визуального ориентира и исчезнет после установки подписи в область.

Изменение размера и положения области для подписанта

1. Нажмите на кнопку **Свойства** на панели с подписантом.
2. Откроется окно **Свойства области**.
3. Внесите необходимые изменения и закройте окно.

Удаление подписанта

Чтобы удалить подписанта из документа нажмите на кнопку **Удалить** , расположенную на панели с его именем.

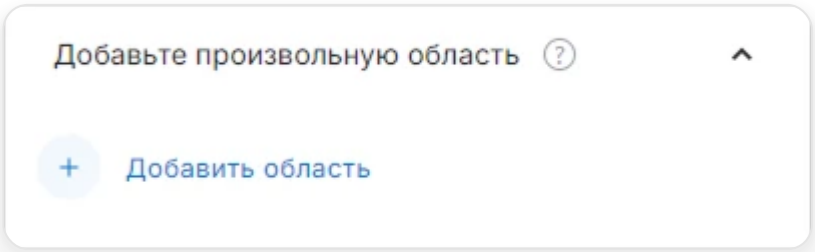
> ⚠️ **Примечание**: Нельзя удалить подписанта в подписанном документе.

8. Произвольная область

> 💡 **Произвольная область** – это область для графического изображения или текста. В области можно разместить свой комментарий, статус или отметку о конфиденциальности документа.

Размещение произвольной области

1. Нажмите кнопку **Добавить область** в блоке **Добавьте произвольную область**.



2. На странице документа появятся пунктирные направляющие. При наведении курсора мыши на пересечении направляющих отобразится схематичный прямоугольник.
3. Наведите курсор мыши в место размещения штампа на странице документа и кликните левой кнопкой мыши. В этом случае размер области будет соответствовать размеру схематичного прямоугольника. Для того, чтобы задать собственный размер области, наведите курсор мыши в место размещения штампа и, зажав левую кнопку мыши, разметьте область нужного размера.

> ⚠️ **Примечание**: После разметки в области появится лейбл с названием области. Данный лейбл служит исключительно для визуального ориентира и исчезнет после настройки внешнего вида штампа.

Изменение размера и положения произвольной области

1. Нажмите на кнопку **Свойства** в блоке **Добавьте произвольную область**.
2. Откроется окно **Свойства области**.

3. Внесите необходимые изменения и закройте окно.

Удаление произвольной области

Чтобы удалить произвольную область из документа нажмите на кнопку **Удалить**  в блоке **Добавьте произвольную область**.

> 💡 **Совет**: Нельзя удалить произвольную область в подписанном документе.

Настройка оформления произвольной области

> 💡 **Примечание**: В произвольную область можно загрузить любое изображение или напечатать текст.

1. Разместите область на странице документа.
2. Нажмите на кнопку **Свойства**  в блоке **Добавьте произвольную область**.
3. В появившемся окне перейдите на вкладку **Внешний вид**.
4. Настройте **Вид области** в блоке **Настройки макета**:
   - Изображение - в области можно будет загрузить любое изображение размером до 10 МБ.
   - Текст - в области можно напечатать любой текст с помощью текстового редактора.
   - Оставить пустым - полномочия по оформлению области будут переданы следующему подписанту.
5. Настройте **Положение области** в блоке **Настройки макета**:
   - Вписать - штамп будет вписан по ширине и высоте в размеченную область.
   - Подогнать область под макет - размер размеченной области будет подогнан под размер изображения или текста.
6. Настройте прозрачность контента произвольной области и отображение границы и фона штампа в блоке **Оформление**.

Возможные ошибки

При возникновении ошибки вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

> ⚠️ **Примечание**: Коды ошибок (0x...) фиксируются для криптопровайдера КриптоПро CSP.

Код ошибки	Ошибка	Рекомендуемые действия
-	**Отсутствует необходимый криптопровайдер. Алгоритм открытого ключа сертификата: ГОСТ Р 34.10-2012 256 бит**	Установите КриптоПро CSP
-	**Отсутствует действующая лицензия КриптоАРМ**	1. Приобретите лицензию КриптоАРМ 2. Активируйте лицензию в настройках программы
0x8009001d	**Отсутствует действующая лицензия КриптоПро CSP**	Установите лицензию КриптоПро CSP
0xc2100140	**Отсутствует лицензия на модуль КриптоПро TSP Client**	Приобретите и установите лицензию TSP Client
0xc2110140	**Отсутствует лицензия на модуль КриптоПро OCSP Client**	Приобретите и установите OCSP Client
-	**Не установлены модули TSP/ OCSP Client**	Установите недостающие модули
-	**Не выбран сертификат подписи**	Выберите сертификат в настройках подписи
-	**Не указан адрес службы TSP**	Введите корректный адрес TSP-сервера
0x80072ee7	**Некорректный адрес службы TSP**	1. Проверьте правильность введенного адреса 2. Убедитесь в доступности сервера
-	**Сертификат не подходит для усовершенствованной подписи**	Выберите подходящий сертификат или измените настройки стандарта подписи
-	**Не указан адрес прокси-сервера**	1. Введите корректный адрес прокси 2. Проверьте параметры сети
-	**Не указан порт прокси-сервера**	1. Укажите правильный порт прокси-сервера 2. Проверьте настройки подключения
0x80072ee6	**Некорректные настройки прокси**	1. Проверьте параметры прокси-сервера 2. Временно отключите прокси для тестирования
-	**Папка для сохранения не найдена**	

Код ошибки	Ошибка	Рекомендуемые действия
		1. Проверьте существование указанной папки 2. Создайте и укажите новую папку для результатов
0x80072ee7	**Нет подключения к интернету**	1. Проверьте сетевое подключение 2. Убедитесь, что брандмауэр не блокирует соединение (Для подписей со штампами)

Инструкции по теме

- Установка сертифицирующей подписи
- Проверка подписи PDF-документа
- Установка личного сертификата
- Создание профиля подписи
- Переключение между профилями подписи

Открыть статью на сайте

Сертифицирующая подпись

- Что такое сертифицирующая подпись
- Сертифицирование документа PDF
- Возможные ошибки

Что такое сертифицирующая подпись

Сертифицирующая подпись (или сертификация PDF) — это особый тип электронной подписи, который не только подтверждает авторство и целостность документа, но и накладывает ограничения на дальнейшие изменения. В отличие от «обычной» подписи, сертифицирующая подпись контролирует, какие именно модификации разрешены в документе после подписания.

При сертификации документа задается перечень разрешенных изменений:

1. Запрет всех изменений:
    - Документ становится "замороженным",
    - Любая попытка редактирования аннулирует подпись.
2. Разрешены отдельные действия:
    - Установка подписи в области, размеченные для подписантов,
    - Настройка внешнего вида произвольной области.

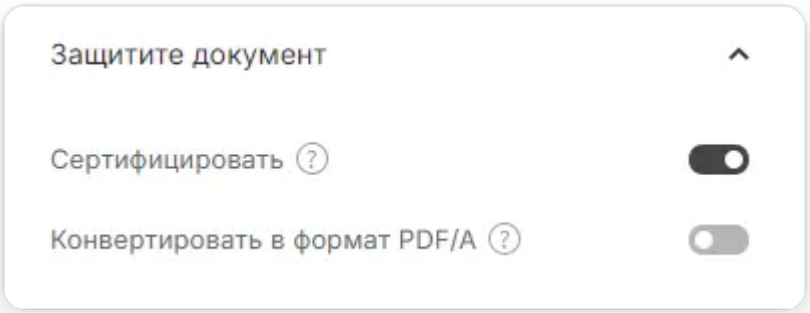
> ⚠️ **Важно**: Поставить сертифицирующую подпись может только первый подписант. Последующие подписи будут «обычными».

Сертифицирование документа PDF

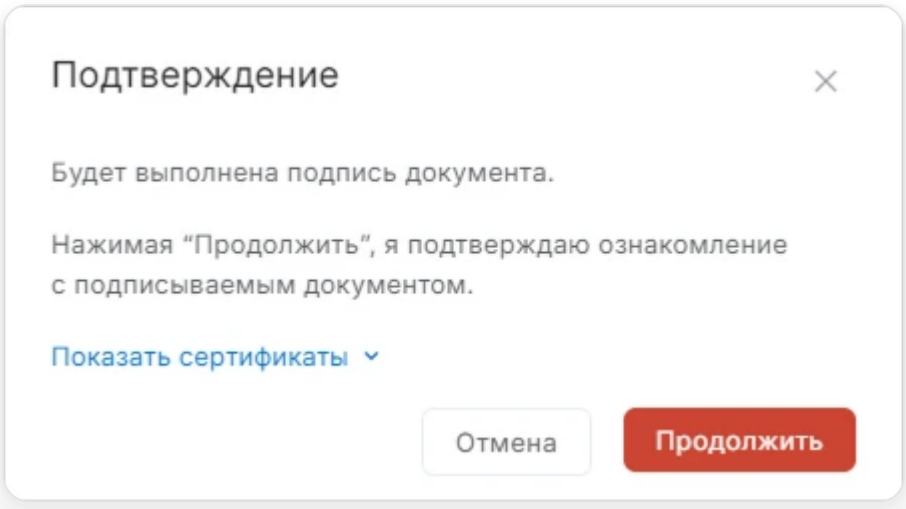
> ⚠️ **Примечание**: Сертификация доступна только для неподписанных документов.

1. Выполните шаги из инструкции Как подписать документ PDF:
    - Шаг 1. Запуск мастера
    - Шаг 2. Добавление документа
    - Шаг 3. Настройки подписи

2. В блоке **Защитите документ** активируйте переключатели:
   - **Сертифицировать** для включения режима защиты от изменений.
   - **Конвертировать в формат PDF/A** для преобразования документа в формат PDF/A с удалением потенциально опасных элементов. Для конвертации потребуется указать дополнительные настройки. Подробнее читайте в инструкции Подпись с конвертацией в PDF/A.



3. Укажите настройки для сохранения результата операции.
4. Нажмите кнопку **Выполнить**.
5. Предоставьте подтверждение на выполнение операции.

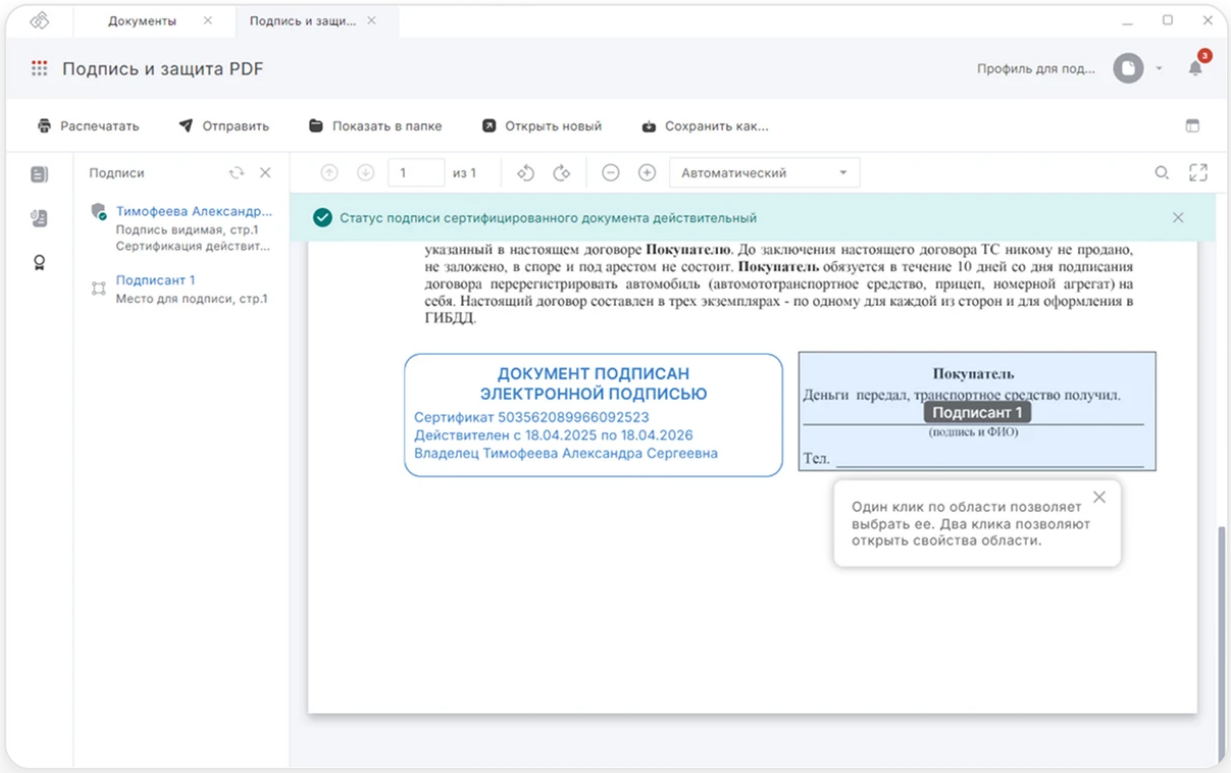


> 🔍 Подробнее про подтверждение читайте в Как подписать документ PDF.

6. Дождитесь окончания операции.
   - Если операция прошла успешно, подписанный файл будет сохранен в соответствии с указанными настройками.
   - Подписанный документ откроется в режиме просмотра и проверки подписи.

> 🔍 Подробнее про проверку подписи читайте в инструкции.

Пример подписанного документа с областью для подписанта:



> 💡**Совет**: В окне с результатами операции вы можете ознакомиться с информацией о подписи, распечатать файл, отправить его по электронной почте или сохранить его в «Архиве».

Возможные ошибки

При возникновении ошибки вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

> 🔍 Полный список ошибок и рекомендации по их устранению можно найти в инструкции Подпись документа PDF.

Инструкции по теме

- Установка подписи в размеченную область
- Проверка подписи PDF-документа
- Установка личного сертификата
- Создание профиля подписи
- Переключение между профилями подписи

Открыть статью на сайте

Подпись с конвертацией в PDF/A

- О конвертации
- Подпись документа с конвертацией в PDF/A
- Возможные ошибки

О конвертации

PDF/A — это международный стандарт (ISO 19005) для долгосрочного архивирования электронных документов, который гарантирует, что документ будет воспроизводиться одинаково на любом устройстве в будущем.

Ключевые особенности:

- Самостоятельность: Все необходимые элементы (шрифты, цветовые профили) встроены в файл,
- Неизменяемость: Запрещены динамические элементы, которые могут изменить отображение,
- Совместимость: Поддержка современных технологий (прозрачность, слои, JPEG2000).

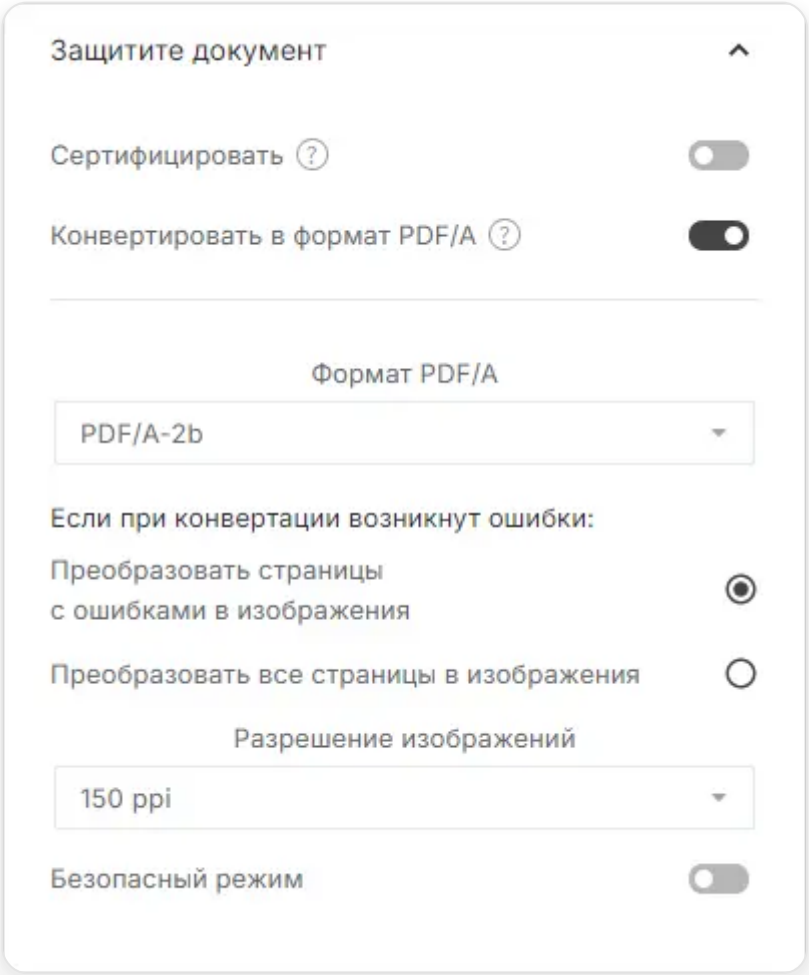
При конвертации документа происходит удаление скриптов, форм и прочие элементов, влияющие на безопасность и целостность документа.

Что удаляется/отключается	Причина
JavaScript и скрипты	Могут изменять отображение
Мультимедиа (аудио, видео)	Не поддерживается стандартом
3D-объекты и интерактивные формы	Нет гарантии долговременной поддержки
Внешние ссылки на ресурсы	Документ должен быть самодостаточным
Шифрование и парольная защита	Мешает верификации содержимого

> ⚠️ **Примечание**:
>
> - Конвертация выполняется только вместе с подписью документа.
> - Конвертация доступна только для неподписанных документов.

Подпись документа с конвертацией в PDF/A

1. Выполните шаги из инструкции Подпись документа PDF:
   - Шаг 1. Запуск мастера
   - Шаг 2. Добавление документа
   - Шаг 3. Настройки подписи
2. В блоке **Защитите документ** активируйте переключатель **Конвертировать в формат PDF/A** для преобразования документа в формат PDF/A с удалением потенциально опасных элементов.



3. Укажите формат конвертации:
   - **PDF/A-2b** — стандарт для архивирования PDF-документов, обеспечивает визуальную совместимость. Документ хранится как PDF, без возможности включать другие файлы.
   - **PDF/A-3b** — расширение формата PDF/A-2b, позволяет встраивать любые файлы (например XML, CSV) внутрь PDF для архивирования вместе с исходными данными.

> ⚠️ **Примечание**: Если вы конвертируете документ с форматом PDF/A-3b в PDF/A-2b, все вложенные файлы внутри документа будут удалены, потому что формат PDF/A-2b не поддерживает встроенные объекты.

4. Выберите вариант действий с документом в случае возникновения ошибок при конвертации:
   - Преобразовать страницы с ошибками в изображения,
   - Преобразовать все страницы в изображения.

> ⚠️ **Примечание**: При преобразовании страниц в изображения размер файла может увеличиться.

5. Выберите разрешение изображений и, при необходимости, активируйте переключатель **Безопасный режим**. В этом режиме страницы обрабатываются последовательно, одна за другой, что снижает нагрузку на систему.
6. Укажите настройки для сохранения результата операции.
7. Нажмите кнопку **Выполнить**.
8. Предоставьте подтверждение на выполнение операции. Подробнее про подтверждение читайте в Подпись документа PDF.
9. Дождитесь окончания операции.
   - Если операция прошла успешно, подписанный файл будет сохранен в соответствии с указанными настройками.
   - Подписанный документ открывается в режиме просмотра и проверки подписи.

> 🔍 Подробнее про проверку подписи читайте в инструкции.
>
> 💡**Совет**: В окне с результатами операции вы можете ознакомиться с информацией о подписи, распечатать файл, отправить его по электронной почте или сохранить его в «Архиве».

Возможные ошибки

При возникновении ошибки вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

🔍 Полный список ошибок и рекомендации по их устранению можно найти в инструкции Подпись документа PDF.

Инструкции по теме

- Установка сертифицирующий подписи
- Установка подписи в размеченную область
- Проверка подписи PDF-документа
- Установка личного сертификата
- Создание профиля подписи
- Переключение между профилями подписи

Открыть статью на сайте

Подпись в размеченную область

- Про размеченные области
- Установка подписи в разметку
- Возможные ошибки

Про размеченные области

Если документ содержит свободные размеченные области для подписантов, то можно поставить подпись в любую из этих областей.

Просмотр доступных областей

Все подготовленные области для подписей отображаются на вкладке **Подписи** в боковом меню мастера **Подпись и защита PDF**.

Здесь вы можете:

- Просмотреть полный список доступных областей
- Определить тип каждой зоны по соответствующей иконке
- Выбрать нужную область для добавления подписи

Типы размеченных областей

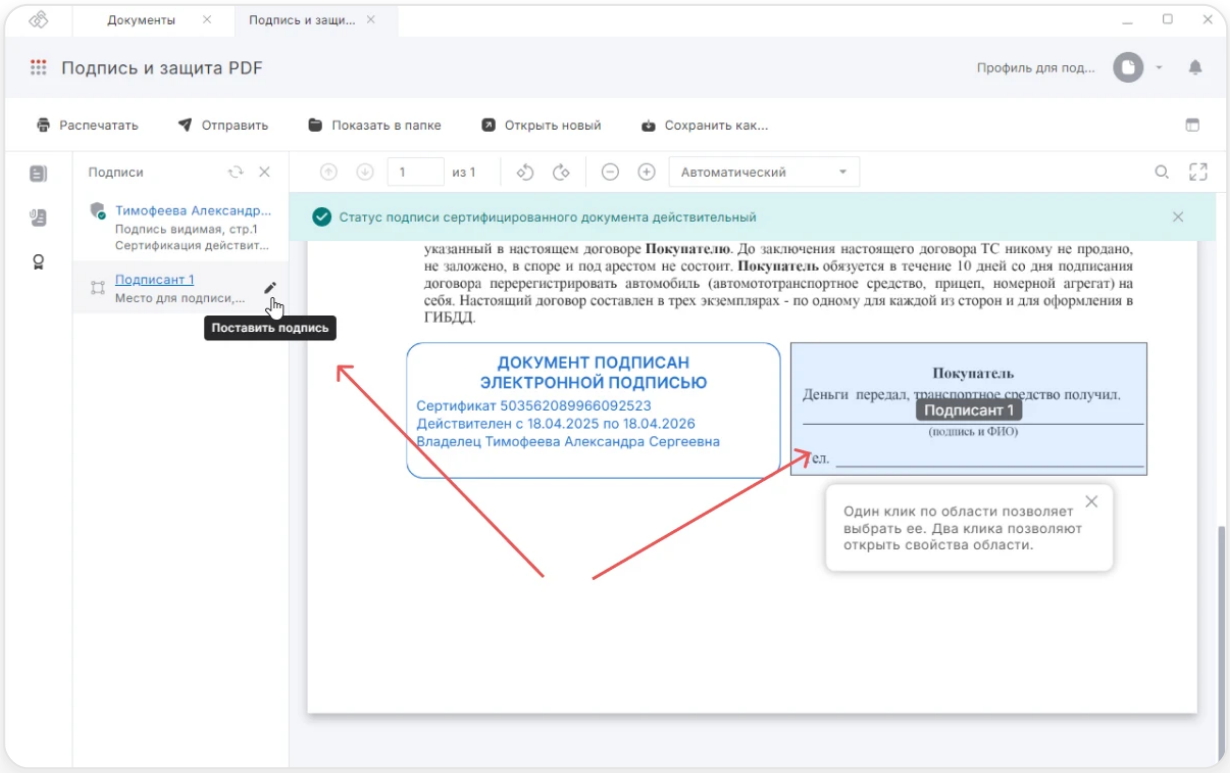
1. **Области для видимых подписей**:
    - Отображаются на странице документа в виде схематической фигуры с именем подписанта,
    - Обозначаются иконкой .
2. **Области для невидимых подписей**:
    - Не имеют визуального отображения на страницах документа,
    - Обозначаются иконкой .

Установка подписи в разметку

1. Выполните шаги из инструкции Как подписать документ PDF:
    - Шаг 1. Запуск мастера
    - Шаг 2. Добавление документа

2. Откройте в боковом меню вкладку **Подписи**.

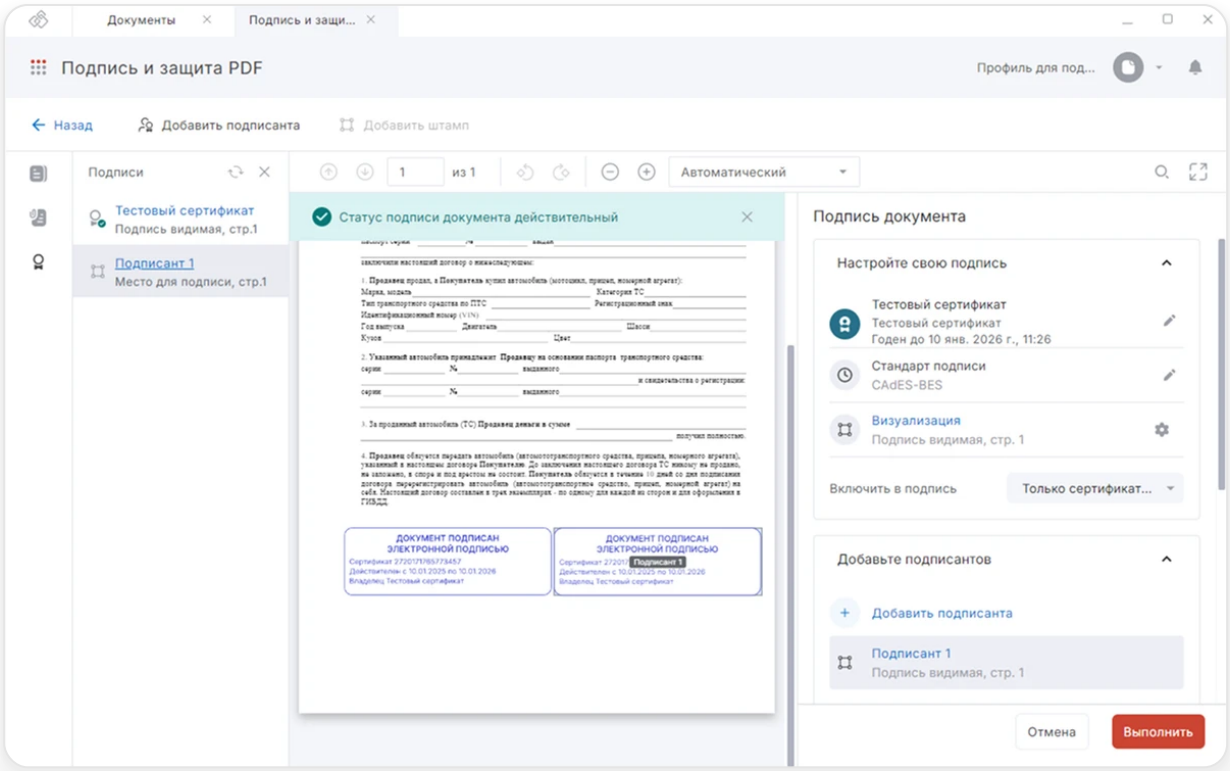
3. Наведите курсор мыши на свободную область и нажмите на кнопку **Поставить подпись** , либо дважды кликните по области на странице документа (если область для видимой подписи).



4. Откроются настройки мастера.

5. Установите настройки подписи по инструкции Шаг 3. Настройки подписи. Если вы устанавливаете подпись в область для видимой подписи, то после выбора личного сертификата в этой области на странице документа появится изображение штампа, которое будет размещено в ней после подписи.

> ⚠️ **Примечание**: Лейбл с именем подписанта служит исключительно для визуального ориентира и исчезнет после подписи документа.

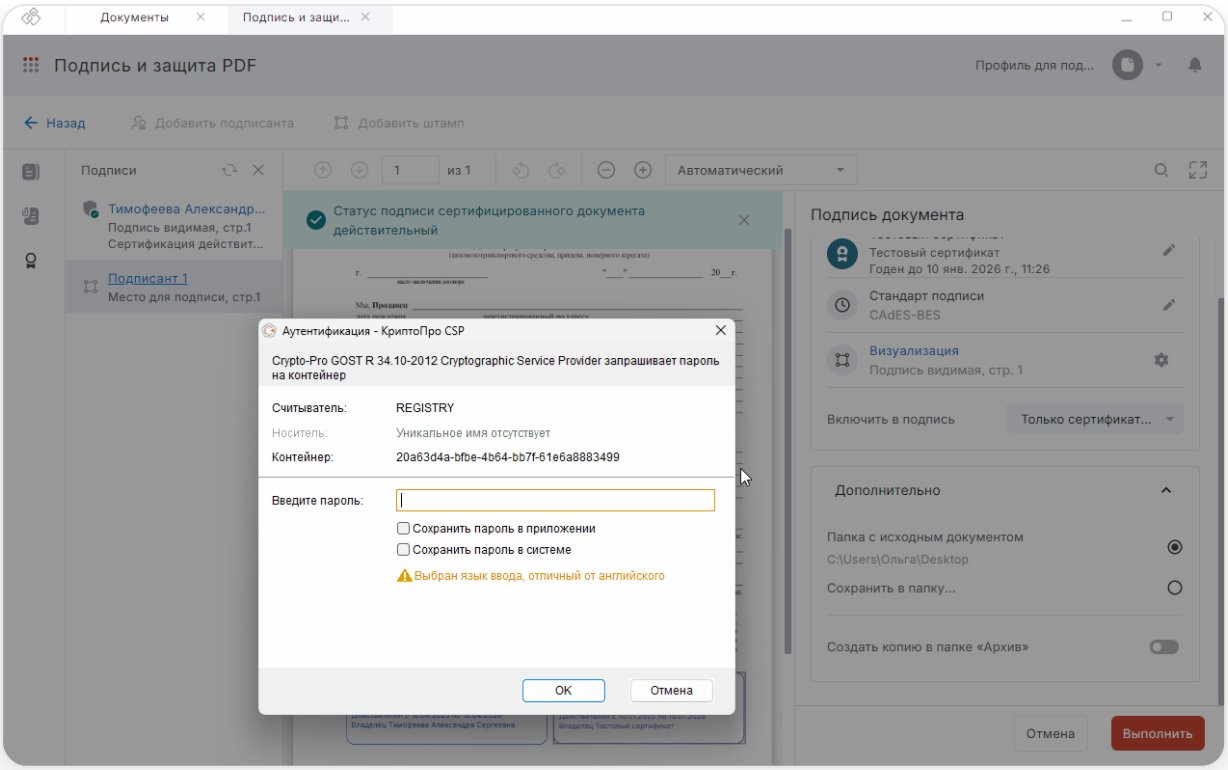


6. Укажите настройки для сохранения результата операции.

7. Нажмите кнопку **Выполнить**.
8. Предоставьте подтверждение на выполнение операции. Подробнее про подтверждение читайте в Как подписать документ PDF.

9. Дождитесь окончания операции.

    - Если операция прошла успешно, подписанный файл будет сохранен в соответствии с указанными настройками.
    - Подписанный документ откроется в режиме просмотра и проверки подписи. Подробнее про проверку подписи читайте в инструкции.



Статичный кадр демонстрации. Открыть анимацию

> 💡**Совет**: В окне с результатами операции вы можете ознакомиться с информацией о подписи, распечатать файл, отправить его по электронной почте или сохранить его в «Архиве».

Возможные ошибки

При возникновении ошибки вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Полный список ошибок и рекомендации по их устранению можно найти в инструкции Подпись документа PDF.

Инструкции по теме

- Установка сертифицирующей подписи
- Проверка подписи PDF-документа
- Установка личного сертификата
- Создание профиля подписи
- Переключение между профилями подписи

Открыть статью на сайте

Проверка подписи

- Проверка подписи документа
- Распространенные проблемы

Проверка подписи документа

> 💡 **С чего начать**: Чтобы оценить, готово ли ваше рабочее место для работы с электронной подписью, воспользуйтесь Проверкой рабочего места.

Шаг 1. Запуск мастера

1. Перейдите в раздел **Документы**.
2. Нажмите **Подпись и защита PDF** в боковом меню раздела **Документы**.
3. Откроется новая вкладка с мастером.

> 💡 **Совет**: Открыть мастер можно с помощью действия **Добавить в** → **Подпись и защита PDF** для файла в папке «Архив», результатах операции или в разделе «Почта».

Шаг 2. Добавление документа

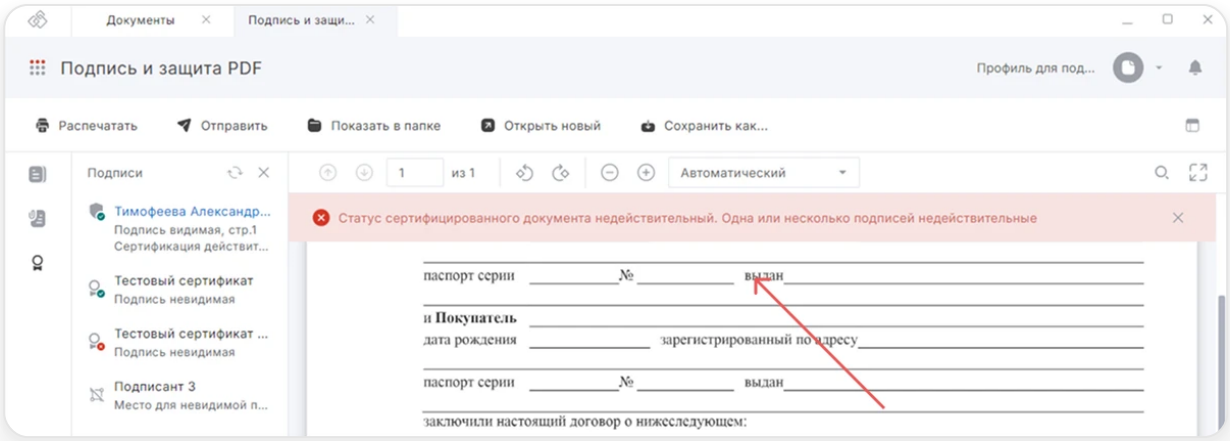
Добавьте документ в мастер одним из способов:

1. Перетащите в окно приложения,
2. Загрузите с помощью кнопки **Загрузить с компьютера**.

Шаг 3. Результаты проверки

Проверка запускается автоматически после добавления документа.

1. Общий статус подписи отображается в виде информера в области просмотра документа.

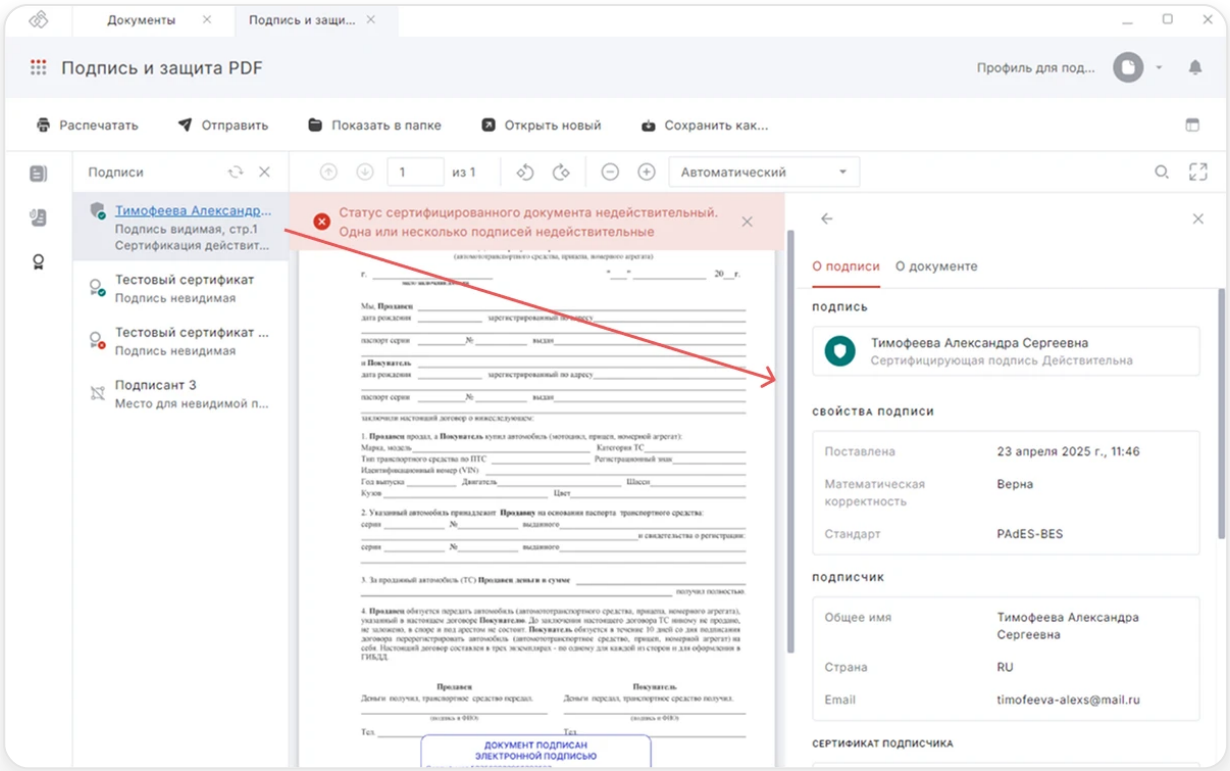


2. Статус каждой из подписей отображается в виде индикатора в боковом меню:
   - зеленая галочка , если подпись действительная,
   - красный крестик, если недействительная.

   Кроме того, различаются иконки для сертифицирующей и «обычной» подписи:

   - «обычная» подпись,
   - сертифицирующая подпись.

3. Наведите курсор на подпись в боковом меню и нажмите на кнопку **Подробно** .
4. В правой части окна отобразится область со сведениями о подписи.



Распространенные проблемы

Причины, по которым подпись может быть недействительной:

Причина	Возможность исправления	Рекомендуемые действия
Отсутствует криптопровайдер с поддержкой ГОСТ Р 34.10-2012	✅ Можно исправить	Установите криптопровайдер КриптоПро CSP и перезапустите приложение КриптоАРМ
Не построилась цепочка сертификации	✅ Можно исправить	Установите корневой и промежуточный сертификаты удостоверяющего центра, который выпустил ваш сертификат
Неактуальный список отзыва (CRL)	✅ Можно исправить	Загрузите актуальный список отозванных сертификатов (CRL)
Срок действия сертификата истёк или сертификат отозван	❌ Невозможно исправить	Запросите новый документ, подписанный действующим сертификатом
Документ изменён после подписания	❌ Невозможно исправить	Запросите оригинальную подписанную версию документа

Инструкции по теме

- Установка сертифицирующей подписи
- Установка подписи в размеченную область
- Проверка подписи PDF-документа
- Установка личного сертификата
- Создание профиля подписи
- Переключение между профилями подписи

Открыть статью на сайте

Выполнение операций в командной строке

- Общая информация
- Подпись
- Шифрование
- Расшифрование
- Проверка подписи

Общая информация

Данное руководство описывает выполнение криптографических операций через интерфейс командной строки (CLI) в операционных системах Windows, Linux и macOS.

Что такое CLI

CLI (Command Line Interface, интерфейс командной строки) — это способ управления приложением с помощью текстовых команд, вводимых через терминал или консоль.

Команды определяют, какие операции выполнить, с какими параметрами и над какими файлами.

В приложении поддержаны операции:

- подпись,
- шифрование,
- расшифрование,
- проверка подписи.

CLI также подходит для автоматизации — выполнения операций без участия пользователя в составе систем обмена и скриптов `.bat` и `.sh`.

> 📌 Ознакомьтесь с примером автоматизации в инструкции.

Важные замечания

- Перед использованием CLI убедитесь, что приложение настроено для работы с электронной подписью.

> 🔍 Подробную информацию о настройке можно найти в инструкции Начало работы.

- Перед вводом команды необходимо указать путь до исполняемого файла. После указания пути до исполняемого файла необходимо поставить пробел, затем вводить команды.
- Все команды и параметры пишутся через пробел.

Синтаксис команд

- `-команда` — команда пишется первой, после пути до исполняемого файла. Далее указываются значения переменных и параметры операции.
- `<текст>` — указываются значения переменной, такие как Серийный номер сертификата, Путь до исходного файла, OID алгоритма шифрования и т.п.
- `[текст]` — необязательные параметры, которые можно как задать, так и не задавать, тогда будут использоваться значения по умолчанию.

Пути к исполняемым файлам

Система	Путь при установке по умочанию
Windows	`"C:\Program Files\CryptoARM 6\cryptoarm6.exe"`
Linux	`/opt/cryptoarm6/cryptoarm6`
macOS	`/Applications/cryptoarm6.app/Contents/MacOS/cryptoarm6`

Подпись

Команда: `sign` или `sig`

Команда позволяет выполнить операцию подписи одного или нескольких файлов.

Если в качестве исходного файла указать уже подписанный документ, то будет добавлена соподпись.

Синтаксис

```
sign  -cert <serial> [-enc DER|BASE64] [-detached] [-save-copy] [-pin <PIN>] [-ext <sign file extention>] [-sign-type <CadesT|CadesA|CadesXLT1> -tsp <tsp-addr> [-ocsp <ocsp-addr>] [-proxy <proxy-addresss> [-proxy-port <port>] [-proxy-login <login>] [-proxy-password <password>]]] <source-file-name>|<source-folder> <encrypted-file-path>|<folder-to-save-signed>
```

Описание команды

Общие параметры подписи

Параметр	Описание	По умолчанию
`--cert <serial>`	Серийный номер сертификата подписи	—
`--standard <type>`	Стандарт подписи CAdES (`CAdES-BES`, `CAdES-T`, `CAdES-A`, `CAdES-XLT1`)	`"CAdES-BES"`
`--detached`	Создать отделённую подпись	Отключено
`--save-copy`	Сохранять копию результата в Архиве	Отключено
`--pin <pin-code>`	ПИН-код ключа сертификата	—
`--enc <DER|BASE-64>`	Формат сохранения подписи	`"DER"`
`--ext <sig|p7s|sgn|sign|bin>`	Расширение файла подписи	`"sig"`
`-f, --force`	Использовать недействительный сертификат без подтверждения	Отключено
`--logcrypto`	Включение лога trusted-crypto	Отключено

Параметры подписи PDF (PAdES)

Параметр	Описание	По умолчанию
`--pades`	Подписать PDF по стандарту PAdES	Отключено
`--overwrite-original-pdf`	Перезаписать исходный файл после подписи	Отключено
`--stamp-width <width>`	Ширина штампа	—
`--stamp-height <height>`	Высота штампа	—
`--stamp-padding-left <padding>`	Отступ слева	—
`--stamp-padding-bottom <padding>`	Отступ снизу	—
`--stamp-color <color>`	Цвет штампа	`#000000`
`--stamp-no-background`	Прозрачный фон под штамп	Отключено
`--stamp-page <number>`	Страница размещения	Последняя
`--stamp-on-all-pages`	Дублировать штамп на всех страницах	Отключено

Параметр	Описание	По умолчанию
`--stamp-mchd <number>`	Добавить номер МЧД в штамп	—
`--stamp-pixel-ratio <ratio>`	Pixel Ratio для рендеринга штампа	`1`

> ⚠️ Ключ `--overwrite-original-pdf` необратимо изменяет исходный файл. Используйте его с осторожностью, особенно в скриптах, где путь к файлу контролируется.
>
> 🚨 Информация в штампе (ФИО, дата, сертификат и т.д.) генерируется автоматически на основе данных вашего сертификата. Настраивается только его визуальное представление, исключение — номер МЧД.

Сетевые параметры

Параметр	Описание	По умолчанию
`--tsp <url>`	Адрес службы метки времени TSP	—
`--ocsp <url>`	Адрес службы OCSP	—
`--proxy <address>`	Адрес прокси-сервера	—
`--proxy-port <port>`	Порт прокси	—
`--proxy-login <login>`	Логин для прокси	—
`--proxy-password <password>`	Пароль для прокси	—

Ввод и вывод

Параметр	Описание	По умолчанию
`--source-file <file>`	Путь к подписываемому файлу	—
`--source-folder <folder>`	Подписать все файлы из папки	—
`--signed-file-path <file>`	Путь для результата подписи	—
`--folder-save-signed <folder>`	Папка для подписанных файлов	—
`-h, --help`	Показать справку	—

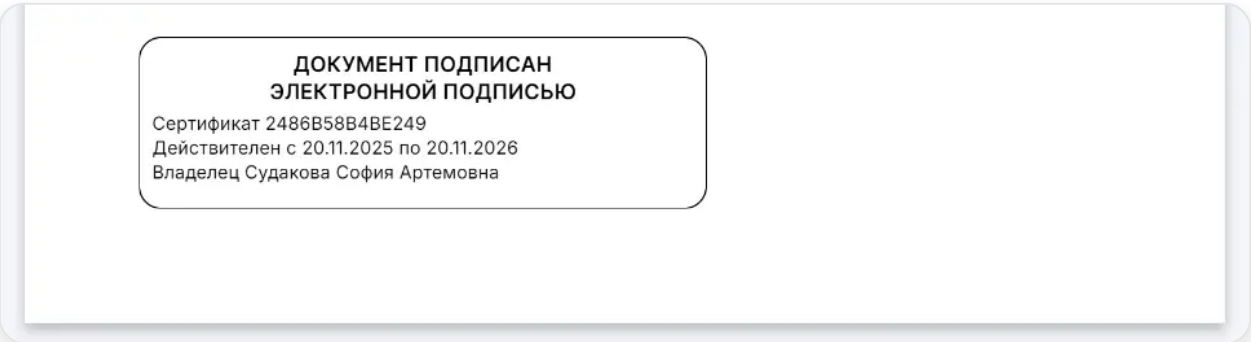
Практические примеры

Пример 1: Подпись со стандартным штампом на последней странице

В этом примере подписывается PDF-файл со штампом размером 100×30 мм, расположенным в 20 мм от левого и нижнего края последней страницы.

```
"C:\Program Files\CryptoARM 6\cryptoarm6.exe" sign \
  --source-file "C:\Doc\Пример.pdf" \
  --cert "5883d78e000300093ab6" \
  --pin "12345678" \
  --pades \
  --stamp-width 100 \
  --stamp-height 30 \
  --stamp-padding-left 20 \
  --stamp-padding-bottom 20
```

Внешний вид штампа:

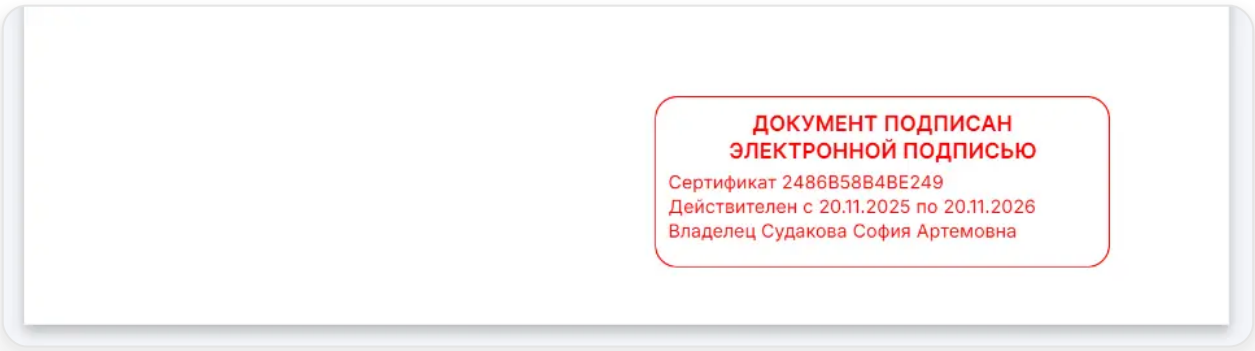


Пример 2: Подпись со штампом красного цвета на всех страницах

В этом примере подписывается PDF-файл со штампом красного цвета. Штамп размещен в правом нижнем углу на каждой странице документа.

```
"C:\Program Files\CryptoARM 6\cryptoarm6.exe" sign \
  --source-file "C:\Doc\Пример.pdf" \
  --cert "5883d78e000300093ab6" \
  --pin "12345678" \
  --pades \
  --stamp-width 80 \
  --stamp-height 30 \
  --stamp-padding-left 110 \
  --stamp-padding-bottom 10 \
  --stamp-color "#FF0000" \
  --stamp-on-all-pages
```

Внешний вид штампа:



Пример 3: Подпись документа с меткой времени

В этом примере подписывается файл со стандартом CAdES-T, который включает метку времени. Файл будет сохранен в формате `.p7s` с кодировкой `BASE-64`. Копия файла будет помещена в папку **Архив** раздела **Документы**.

```
"C:\Program Files\CryptoARM 6\cryptoarm6.exe" sign \
  --source-file "C:\Documents\Example.pdf" \
  --cert "5883d78e000300093ab6" \
  --pin "12345678" \
  --standard "CAdES-T" \
  --tsp "https://example.com/tsp/tsp.srf" \
  --enc "BASE-64" \
  --ext "p7s" \
  --save-copy \
```

Шифрование

Команды: `encrypt` или `enc`

Команда позволяет выполнить шифрование одного или нескольких файлов в адрес одного или нескольких сертификатов.

Синтаксис

```
encrypt --cert <серийный номер сертификата> [--enc DER|BASE64][--alg <alg-oid>] [--delete-source][--save-copy] [--ext <encrypted file extension>] --source-file <путь к файлу>|--source-folder <путь к папке> --encrypted-file-path <путь к файлу с новым именем для сохранения результата>|--folder-save-encrypted <путь к папке для сохранения результата>
```

Описание команды

Параметр	Описание	Значение по умолчанию
`--cert <serial...>`		—

Параметр	Описание	Значение по умолчанию
	Серийный номер сертификата подписи (можно указать несколько)	
`--alg <alg-oid>`	OID алгоритма шифрования	`"1.2.643.2.2.21"`
`--delete-source`	Удаление исходного файла после шифрования	Отключено
`--save-copy`	Сохранение копии результата в Архиве	Отключено
`--ext <enc|p7m|p7e|pem>`	Расширение создаваемого шифрованного файла	`"enc"`
`--enc <DER|BASE-64>`	Кодировка шифруемого файла	`"DER"`
`--logcrypto`	Включает лог trusted-crypto	Отключено
`-f, --force`	Автоматическое согласие на использование недействительных сертификатов	Отключено
`--source-file <path-file>`	Путь к файлу для шифрования	—
`--encrypted-file-path <path-file>`	Путь к файлу для сохранения результата шифрования	—
`--folder-save-encrypted <path-folder>`	Путь к папке для сохранения зашифрованных файлов	—
`--source-folder <path-folder>`	Путь к папке с файлами для шифрования	—
`-h, --help`	Вывод справки команды	—

Практический пример

В этом примере шифруется файл `Example.txt` с использованием сертификата с серийным номером `5883d78e000300093ab6`. Результат шифрования будет сохранен в файл `Encrypted_Example.enc`. Исходный файл будет удален, а копия зашифрованного файла сохранится в папку **Архив** раздела **Документы**.

```
"C:\Program Files\CryptoARM 6\cryptoarm6.exe" encrypt \
  --cert "5883d78e000300093ab6" \
  --enc "DER" \
  --alg "1.2.643.2.2.21" \
  --delete-source \
  --ext "enc" \
  --save-copy
  --source-file "C:\Documents\Example.txt" \
  --encrypted-file-path "C:\Documents\Encrypted_Example.enc"
```

Расшифрование

Команды: `decrypt` или `dec`

Команда позволяет выполнить расшифрование одного или нескольких зашифрованных файлов.

Синтаксис

```
decrypt [-pin <PIN>] [-save-copy] <source-file-name>|<source-folder> <encrypted-file-path>|
<folder-to-save-decrypted>
```

Описание команды

Параметр	Описание	Значение по умолчанию
`--save-copy`	Сохранение копии результата в Архиве	Отключено
`--logcrypto`	Включает лог trusted-crypto	Отключено
`--pin <pin-code>`	Пин-код ключа расшифрования	-
`--source-file <path-file>`	Путь к файлу для расшифрования	-
`--source-folder <path-folder>`	Путь к папке с файлами для расшифрования	-
`--decrypted-file-path <path-file>`	Путь для сохранения расшифрованного файла	-
`--folder-save-decrypted <path-folder>`	Путь к папке для сохранения результатов расшифрования	-
`-h, --help`	Вывод справки команды	-

Практический пример

В этом примере расшифровывается файл `Encrypted_Example.enc`. Для сертификата шифрования используется ПИН-код `12345678`. Расшифрованный результат сохраняется в `C:\Documents\`.

```
"C:\Program Files\CryptoARM 6\cryptoarm6.exe" decrypt \
  --pin "12345678" \
  --source-file "C:\Documents\Encrypted_Example.enc" \
  --decrypted-file-path "C:\Documents\Decrypted_Example.txt"
```

Проверка подписи

Команды:

- `verify` или `ver`
- `verify_ts` или `vts` - проверка штампов времени из подписи

Команда позволяет выполнить проверку одной или нескольких подписей, либо штампов времени в файле подписи. Есть возможность сохранения отчёт о проверке в отдельный файл в формате `pdf` или `json`.

Синтаксис

```
verify [-save-report|-r [<report-file>]] <source-file-name>|<source-folder>
```

```
verify_ts [-save-report|-r [<report-file>]] <source-file-name>|<source-folder>
```

Описание команды

Параметр	Описание	Значение по умолчанию
`-r-pdf`, `--save-report-pdf [report-folder]`	Сохранение отчёта в формате PDF	Отключено
`-r-json`, `--save-report-json [report-file-path]`	Сохранение отчёта в формате JSON	Отключено
`--document <original-file>`	Путь к исходному файлу для откреплённой подписи	-
`--logcrypto`	Включение лога trusted-crypto	Отключено
`--source-file <source-file-path>`	Путь к файлу подписи для проверки	-
`--source-folder <source-folder-path>`	Путь к папке с подписями для проверки	-
`-h`, `--help`	Вывод справки по команде	-

Практический пример

В этом примере выполняется проверка подписи файлов в папке `C:\Foldername` с сохранением отчета о проверке в формате `pdf` в папку с проверяемыми файлами.

```
"C:\Program Files\CryptoARM 6\cryptoarm6.exe" ver --source-folder C:\Foldername -r-pdf
```

Открыть статью на сайте

Пример автоматизации

- Пример
- Особенности скрипта
- Использование

Пример

Рассмотрим пример простого скрипта для проверки подписанных документов в папке с созданием общего отчета о проверке. Общий отчет о проверке сохраняется в формате JSON в ту же папку.

> 🚨 **Важно:** Во время проверки для каждого документа создаются JSON-файлы с отчетами. После завершения проверки скрипт удаляет эти файлы и формирует общий сводный отчет. Удалите строку `del /q "reportfile*.json"`, если необходимо сохранить эти отчеты.

```
set "SCRIPT_DIR=%~dp0"
"C:\Program Files\CryptoARM 6\cryptoarm6.exe" ver --source-folder %SCRIPT_DIR% -r-json
@echo off
setlocal enabledelayedexpansion

:: Настройки
set "log_file=signature_check_%date:~-4,4%%date:~-7,2%%date:~-10,2%_%time:~0,2%
%time:~3,2%.log"
set "valid_count=0"
set "invalid_count=0"
set "valid_files="
set "invalid_files="

:: Создаем лог-файл
echo Проверка JSON-файлов на валидность подписи [%date% %time%] > "%log_file%"
echo. >> "%log_file%"

:: Проверяем файлы
echo Анализируем JSON-файлы...
echo Анализируем JSON-файлы... >> "%log_file%"
echo. >> "%log_file%"

for %%F in (*.json) do (
    echo Обработка файла: %%F
    echo Обработка файла: %%F >> "%log_file%"

    find /i """signValid"":true" "%%F" > nul
    if !errorlevel! equ 0 (
        set /a "valid_count+=1"
        set "valid_files=!valid_files!"%%F" "
```

```
        echo   Найдена VALID подпись >> "%log_file%"
        echo [VALID] %%F
    ) else (
        find /i """signValid"":false" "%%F" > nul
        if !errorlevel! equ 0 (
            set /a "invalid_count+=1"
            set "invalid_files=!invalid_files!"%%F" "
            echo   Найдена INVALID подпись >> "%log_file%"
            echo [INVALID] %%F
        ) else (
            echo   Не найдена информация о подписи >> "%log_file%"
            echo [NO DATA] %%F
        )
    )
    echo. >> "%log_file%"
)

:: Выводим результаты
echo.
echo ============ ИТОГИ ============
echo. >> "%log_file%"
echo ============ ИТОГИ ============ >> "%log_file%"

echo Валидных подписей:   !valid_count!
echo Валидных подписей:   !valid_count! >> "%log_file%"

echo Невалидных подписей: !invalid_count!
echo Невалидных подписей: !invalid_count! >> "%log_file%"

echo.
echo. >> "%log_file%"

echo ===== Файлы с VALID подписями: =====
echo ===== Файлы с VALID подписями: ===== >> "%log_file%"
for %%F in (!valid_files!) do (
    echo %%~F
    echo %%~F >> "%log_file%"
)

echo.
echo. >> "%log_file%"

echo ===== Файлы с INVALID подписями: ===
echo ===== Файлы с INVALID подписями: === >> "%log_file%"
for %%F in (!invalid_files!) do (
    echo %%~F
    echo %%~F >> "%log_file%"
)

echo.
echo. >> "%log_file%"

echo Лог сохранен в файл: %log_file%
echo.
del /q "reportfile*.json"
pause
```

> ⚠️ **Примечание**: При необходимости замените путь к исполняемому файлу: `"C:\Program Files\CryptoARM 6\cryptoarm6.exe"`.

Особенности скрипта

1. **Инициализация и подготовка**
   - При запуске скрипт автоматически определяет свою рабочую директорию (`%~dp0`).
   - Создается лог-файл с именем: (`signature_report.log`).
   - Инициализируются счетчики для подсчета действительных и недействительных подписей.
2. **Процесс проверки файлов**
   - Скрипт анализирует каждый промежуточный JSON-файл с отчетом, который создается для каждого подписанного документа.
   - Выполняется поиск строк:
     - `"signValid":true` - признак действительной подписи
     - `"signValid":false` - признак недействительной подписи
3. **Формирование отчета**
   - После проверки всех файлов скрипт генерирует итоговый отчет, содержащий:
     - Общее количество проверенных файлов
     - Количество файлов с действительными подписями
     - Количество файлов с недействительными подписями
   - Отчет сохраняется в том же каталоге, что и скрипт.
4. **Очистка и завершение**
   - Автоматически удаляются JSON-файлы с отчетами, которые создаются для каждого документа.

Использование

1. Сохраните код в файл с расширением `.bat`.
2. Поместите этот файл в папку с подписанными файлами.
3. Запустите двойным кликом.

Открыть статью на сайте

Открытие документа

- Основные принципы
- Пошаговая инструкция
- Возможные ошибки

Основные принципы

Документы открываются в программе, ассоциированной с их расширением в операционной системе.

Для работы с защищёнными файлами учитывайте следующие особенности:

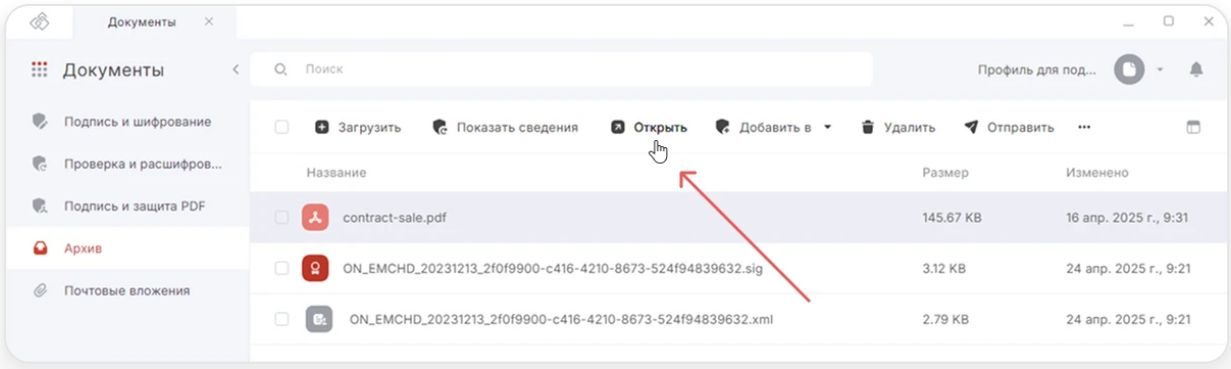
- Подписанные и зашифрованные документы открываются в оригинальном виде,
- Зашифрованные документы требуют предварительного расшифрования.

> 🔐 **Важное условие**: Для открытия зашифрованных документов в хранилище «Личные сертификаты» должен присутствовать сертификат с закрытым ключом, который использовался при шифровании.
>
> 💡 **С чего начать**: Чтобы оценить, готово ли ваше рабочее место для работы с электронной подписью, воспользуйтесь Проверкой рабочего места.

Пошаговая инструкция

Способ 1: Через интерфейс приложения

1. Выделите документ в одном из разделов:
    - Папка **Архив** или **Почтовые вложения**,
    - Мастер **Подпись и шифрование**,
    - Мастер **Проверка и расшифрование**.
2. Нажмите кнопку **Открыть** на панели инструментов.



Способ 2: Быстрое открытие

Дважды кликните по названию файла в списке документов.

Возможные ошибки

При возникновении ошибки вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

> ⚠️ **Примечание**: Коды ошибок (0x...) фиксируются для криптопровайдера КриптоПро CSP.

Код ошибки	Ошибка	Описание	Рекомендуемые действия
0x80092004	Не удалось расшифровать файл	Отсутствует сертификат, в адрес которого выполнено шифрование	1. Проверьте наличие в хранилище "Личные сертификаты" нужного сертификата 2. Убедитесь, что сертификат содержит закрытый ключ 3. Проверьте, что это именно тот сертификат, которым производилось шифрование
-	Не удалось расшифровать файл (для файлов, зашифрованных в адрес сертификатов с алгоритмами ГОСТ)	Отсутствует лицензия КриптоАРМ	1. Приобретите лицензию КриптоАРМ 2. Активируйте лицензию в настройках программы
-	Не удалось расшифровать файл	Отсутствует КриптоПро CSP	

Код ошибки	Ошибка	Описание	Рекомендуемые действия
			Установите криптопровайдер КриптоПро CSP и перезапустите приложение КриптоАРМ
0x8009001d	Не удалось расшифровать файл	Отсутствует действующая лицензия КриптоПро CSP	Установите лицензию КриптоПро CSP
-	Не удалось найти исходный файл для подписи	Исходный документ для файла открепленной подписи не найден или имеет другое название	1. В боковой панели нажмите **Указать путь к файлу** для выбора исходного документа 2. Укажите путь к исходному документу.

Инструкции по теме

- Подпись документа со стандартом CAdES
- Подпись документа со стандартом PAdES
- Шифрование документа
- Проверка подписи документа
- Установка личного сертификата

Открыть статью на сайте

Просмотр сведений

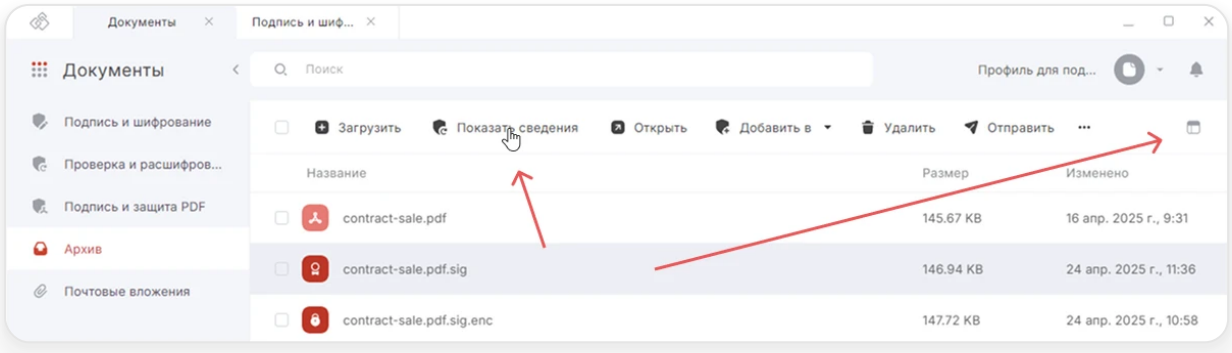
- Просмотр сведений о документе
- Просмотр печатной формы МЧД
- Дополнительные действия
- Возможные ошибки

В приложении КриптоАРМ можно просмотреть информацию о документе и его подписях не только в мастере «Проверка и расшифрование», но и в мастере «Подпись и шифрование», а также в папках «Архив» и «Почтовые вложения».

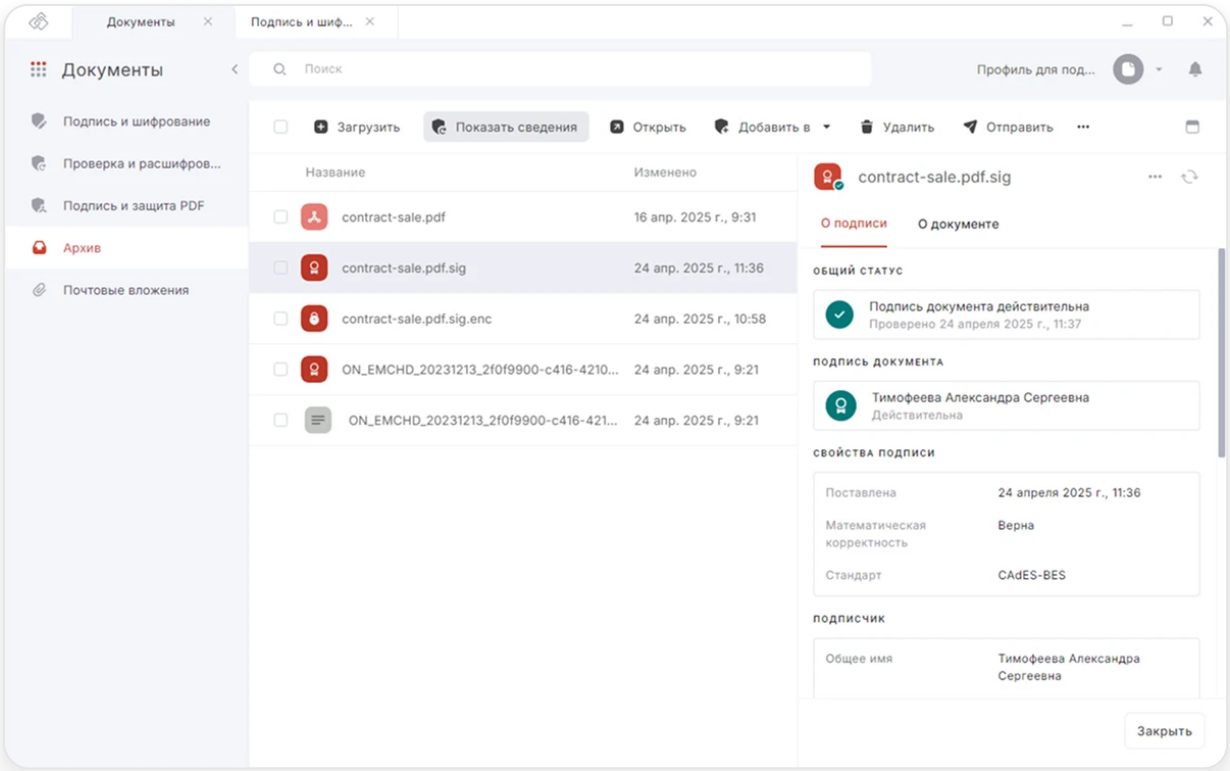
> 💡 **С чего начать**: Чтобы оценить, готово ли ваше рабочее место для работы с электронной подписью, воспользуйтесь Проверкой рабочего места.

Просмотр сведений о документе

1. Выделите документ в одном из разделов:
   - Папка **Архив** или **Почтовые вложения**,
   - Мастер **Подпись и шифрование**,
   - Мастер **Проверка и расшифрование**.
2. Нажмите на кнопку **Показать сведения** или кнопку **Подробно** на панели действий.



3. Справа от списка писем откроется область со сведениями:
   - Нажмите на вкладку **О подписи** для просмотра сведений о подписи документа.
   - Нажмите на вкладку **О документе** для просмотра сведений о документе,

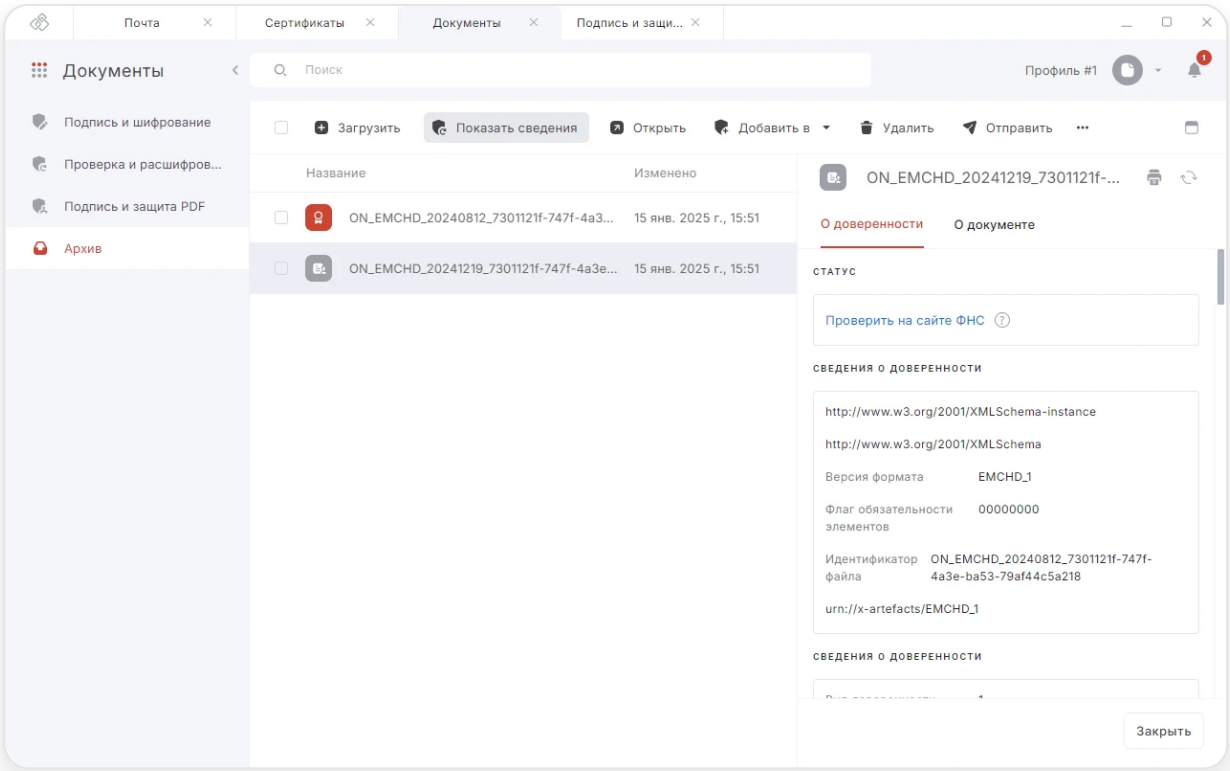


> 💡 **Совет**: Если подпись по какой-то причине не проходит проверку или считается недействительной, ознакомьтесь с инструкцией Распространенные проблемы.

Просмотр печатной формы МЧД

> **Печатная форма МЧД** — удобное для чтения представление машиночитаемой доверенности.

1. Выделите файл МЧД с расширением .xml в одном из разделов:
   - Папка **Архив** или **Почтовые вложения**,
   - Мастер **Подпись и шифрование**,
   - Мастер **Проверка и расшифрование**.
2. Нажмите на кнопку **Показать сведения** или кнопку **Подробно** на панели действий.
3. Справа от списка писем откроется область со сведениями:
   - Нажмите на вкладку **О доверенности** для просмотра печатной формы доверенности.
   - Нажмите на вкладку **О документе** для просмотра сведений о документе,



Дополнительные действия

Обновление сведений о подписи

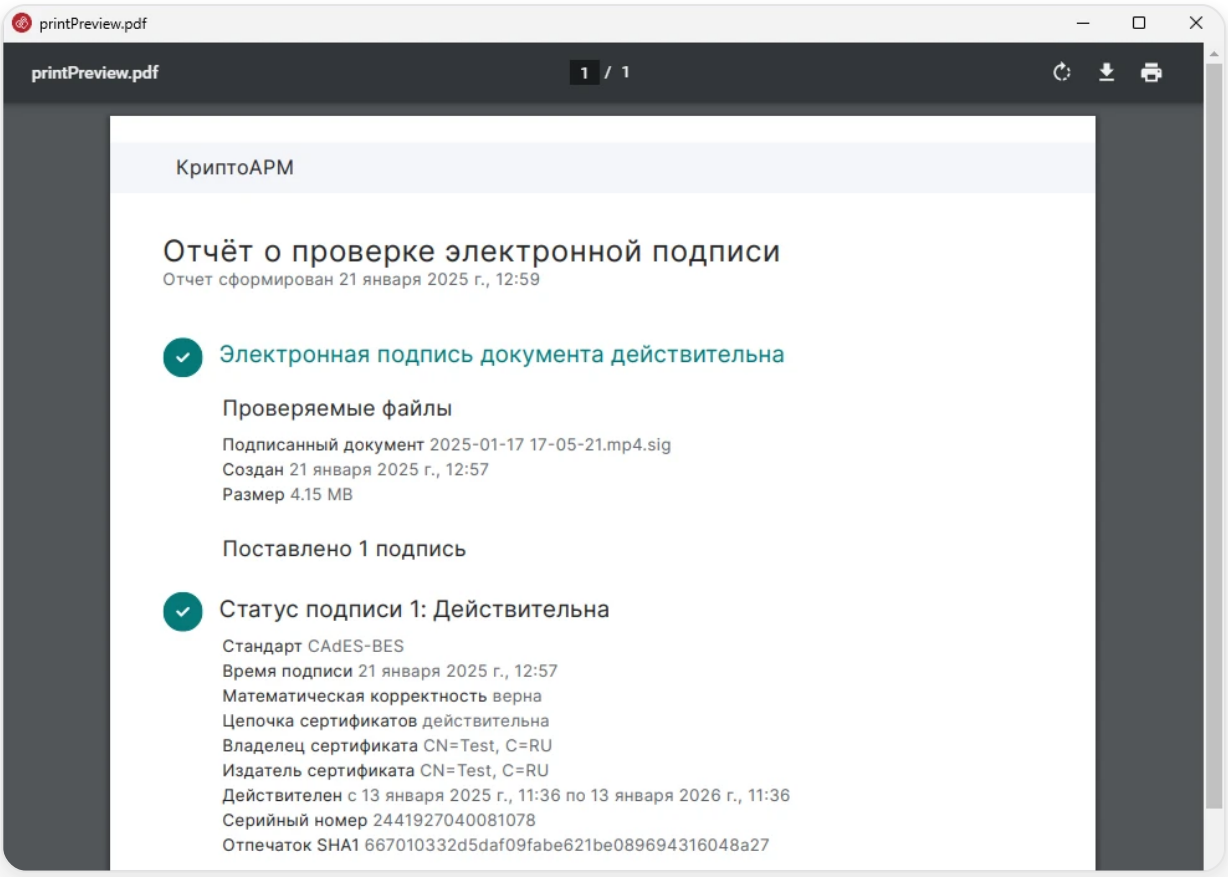
В некоторых случаях, например, при установке корневого или промежуточного сертификата, может потребоваться повторная проверка подписи документа.

1. Откройте сведения для подписанного документа по инструкции.
2. Перейдите на вкладку **О подписи**.
3. Нажмите на кнопку **Обновить** .

Сведения о подписи будут обновлены.

Печать сведений о подписи

1. Откройте сведения для подписанного документа по инструкции.
2. Перейдите на вкладку **О подписи**.
3. Нажмите на кнопку **Распечатать отчет** .
4. Откроется окно с отчетом о проверке электронной подписи.



Отчет можно распечатать или скачать на устройство.

Создание печатной формы для PDF-документа

Для подписанных PDF-документов можно создать копию с графическим штампом подписи. В такой копии присутствует только визуальное представление штампа, а сама электронная подпись отсутствует.

> 📌 **Важно понимать!** Печатная форма документа предназначена для визуального ознакомления с его содержанием и подтверждения факта подписания. Однако она не имеет юридической силы оригинала, поскольку не содержит электронной подписи и связанных с ней криптографических данных.

Чтобы создать печатную форму при просмотре сведений о документе:

1. Откройте сведения для подписанного PDF-документа по инструкции.
2. Перейдите на вкладку **О подписи**.
3. Вызовите меню действий по клику на кнопку **Еще** ••• .
4. Выберите действие **Создать печатную форму со штампом**.

Печатная форма сохранится в папку, в которой находится подписанный документ.

🚨 Вы можете создать печатную форму при подписании PDF-документа. Читайте подробнее в инструкции Подпись с созданием печатной формы.

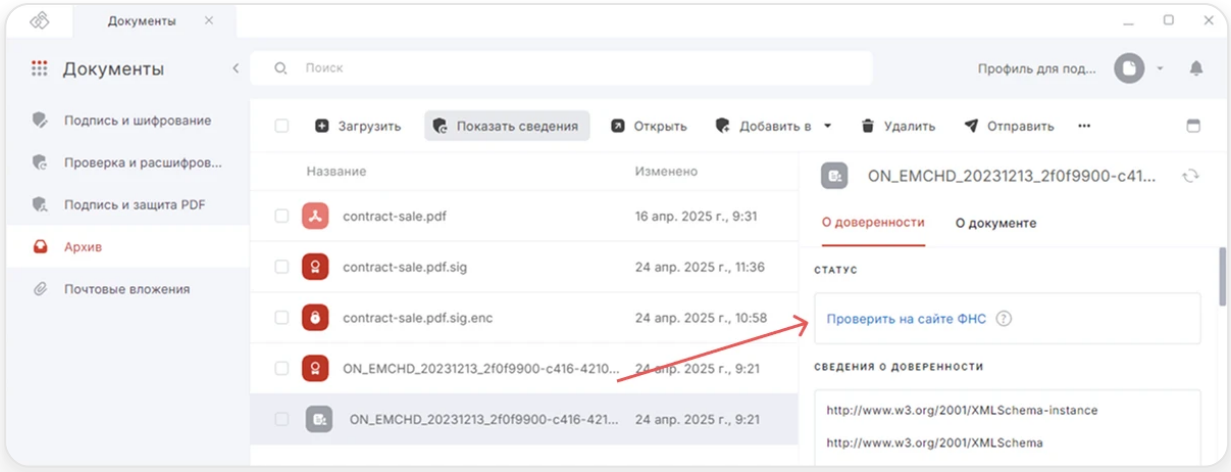
Печать МЧД

1. Откройте сведения о файле МЧД с расширением .xml по инструкции.
2. Перейдите на вкладку **О доверенности**.
3. Нажмите на кнопку **Печать** .
4. Откроется окно с печатной формой МЧД.

МЧД можно распечатать или скачать на устройство.

Проверка статуса МЧД

1. Откройте сведения о файле МЧД с расширением .xml по инструкции.
2. Перейдите на вкладку **О доверенности**.
3. В блоке **Статус** нажмите на кнопку **Проверить на сайте ФНС**.



В браузере по умолчанию откроется сайт ФНС со статусом доверенности.

Возможные ошибки

При возникновении ошибки вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Описание	Рекомендуемые действия
Не удалось найти исходный файл для подписи		

Ошибка	Описание	Рекомендуемые действия
	Исходный документ для файла откреплённой подписи не найден или имеет другое название	1. В боковой панели нажмите **Указать путь к файлу** для выбора исходного документа 2. Укажите путь к исходному документу.

Инструкции по теме

- Подпись документа со стандартом CAdES
- Подпись документов со стандартом PAdES
- Шифрование документа
- Проверка подписи документа
- Установка личного сертификата

Открыть статью на сайте

Загрузка в Архив

- Для чего нужна папка «Архив»?
- Загрузка документов в «Архив»
- Настройка автоматического сохранения в папку «Архив»

Для чего нужна папка «Архив»?

Папка **Архив** предназначена для безопасного и удобного хранения подписанных, зашифрованных и других обработанных документов.

Какие файлы можно хранить в «Архиве»?

- Подписанные файлы,
- Зашифрованные файлы,
- Файлы машиночитаемой доверенности,
- Другие резервные копии важных документов.

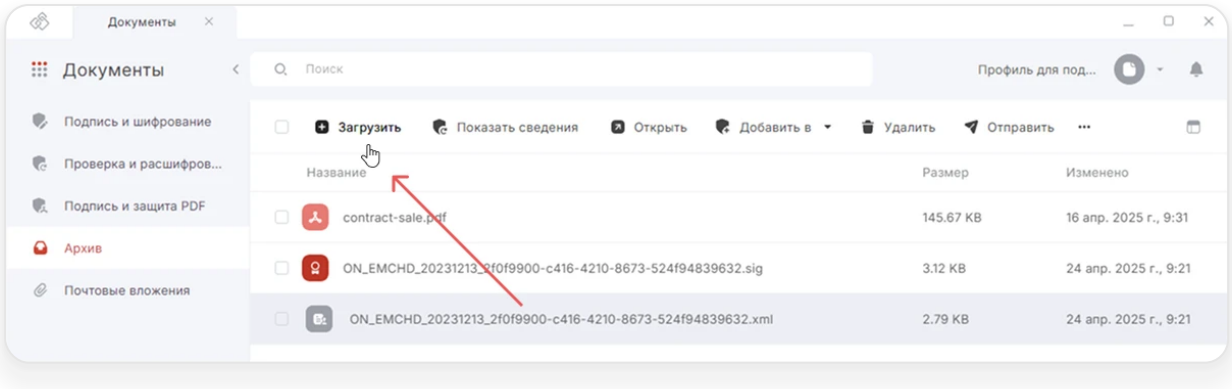
Основные функции

- ✅ Помогает избежать потери документов,
- ✅ Быстрый доступ к ранее обработанным документам,
- ✅ Использование документов без повторной загрузки,
- ✅ Отправка напрямую из «Архива» в качестве вложения в электронное письмо.

Загрузка документов в «Архив»

> ⚠️ **Примечание**: Загружаемые файлы учитываются в общем объеме данных приложения.

1. Перейдите в раздел **Документы** → **Архив**.
2. Добавьте файлы одним из способов:
    - Перетащите один или несколько файлов в окно приложения,
    - Нажмите **Загрузить** на панели действий и выберите файлы вручную.



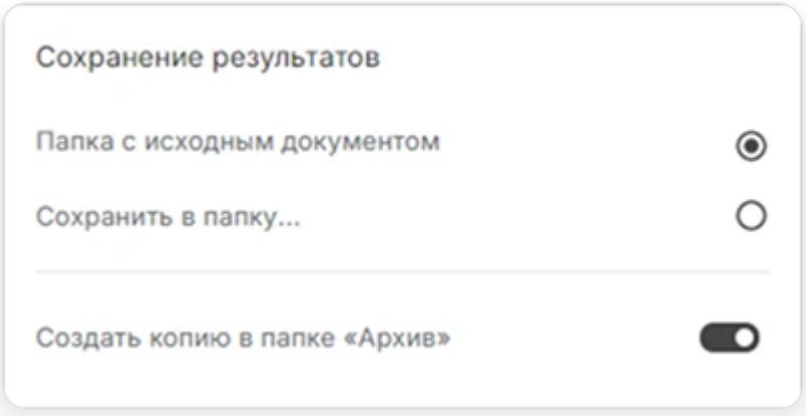
После загрузки документы автоматически появятся в списке.

> 💡 **Совет**: Вы можете перетаскивать как файлы, так и папки. Все содержимое вложенных папок тоже будет добавлено в **Архив**.

Настройка автоматического сохранения в папку «Архив»

Включение автосохранения результатов операций

1. При выполнении операции в мастерах:
    - **Подпись и шифрование**
    - **Подпись и защита PDF**
2. В блоке **Сохранение результатов** активируйте опцию **Создать копию в папке «Архив»**.



КриптоАРМ будет автоматически сохранять все результирующие файлы в указанную папку.

> 💡 Совет: Чтобы опция **Создать копию в папке «Архив»** активировалась автоматически, настройте ее в профиле подписи.

Особенности работы

1. При создании отсоединённой подписи в **Архив** сохраняется:
    - Файл подписи,
    - Копия исходного документа.
2. В **Архив** не сохраняются промежуточные файлы, создаваемые в результате выполнения операции.

Инструкции по теме

- Подпись документа со стандартом CAdES
- Подпись документа со стандартом PAdES
- Шифрование документа
- Проверка подписи документа
- Установка личного сертификата

Открыть статью на сайте

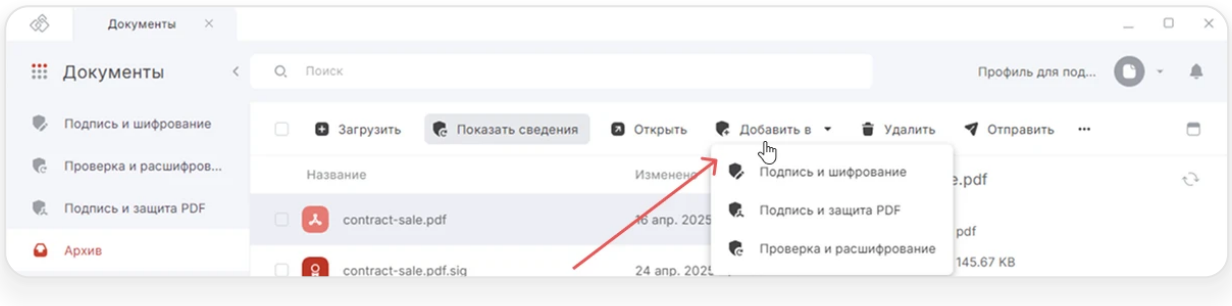
Прочие действия

- Добавление в мастер
- Отправление по почте
- Показать в папке
- Удаление документа

Добавление в мастер

Документы, хранящиеся в папке **Архив**, можно открыть в одном из мастеров с помощью действия **Добавить в**.

1. Перейдите в раздел **Документы** → папка **Архив**.
2. Выделите один или несколько документов.
3. Нажмите на кнопку **Добавить в** на панели действий.
4. Откроется меню со списком мастеров, доступных для выбранного документа:
    - Подпись и шифрование,
    - Проверка и расшифрование,
    - Подпись и защита PDF (доступно для документов с расширением PDF)
5. Выберите мастер, в котором необходимо открыть документ.



Отправление по почте

> ⚠️ **Примечание**: Для отправки профилей подписи по почте в приложении должен быть подключен почтовый аккаунт.

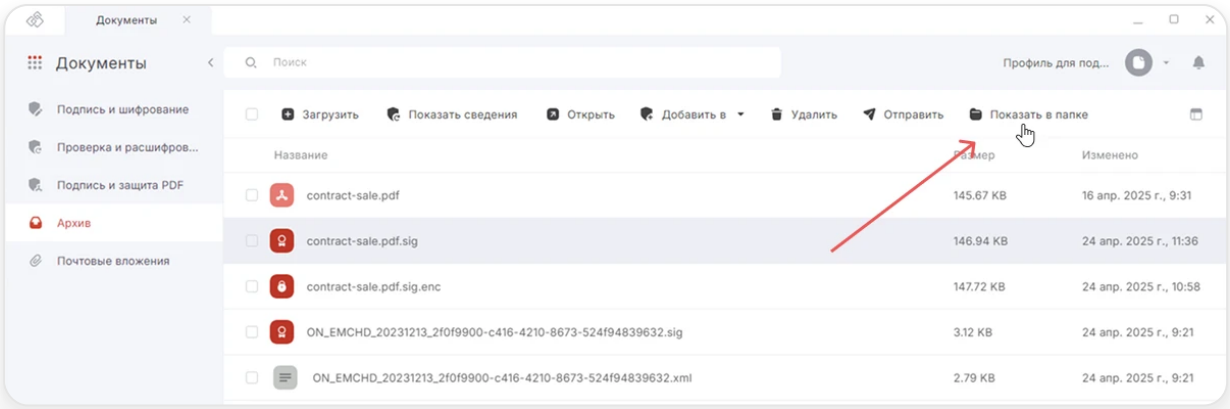
1. Выделите один или несколько документов в одном из разделов:
    - Папка **Архив**,
    - Мастер **Подпись и шифрование** (в окне с результатами операций),
    - Мастер **Проверка и расшифрование** (в окне с результатами операций).
2. Нажмите на кнопку **Отправить** на панели действий.
3. Откроется вкладка с новым письмом, в которой выбранные файлы будут добавлены во вложения.
4. Заполните обязательные поля и отправьте письмо.

Показать в папке

Функция **Показать в папке** позволяет быстро найти физическое расположение документа в файловой системе компьютера.

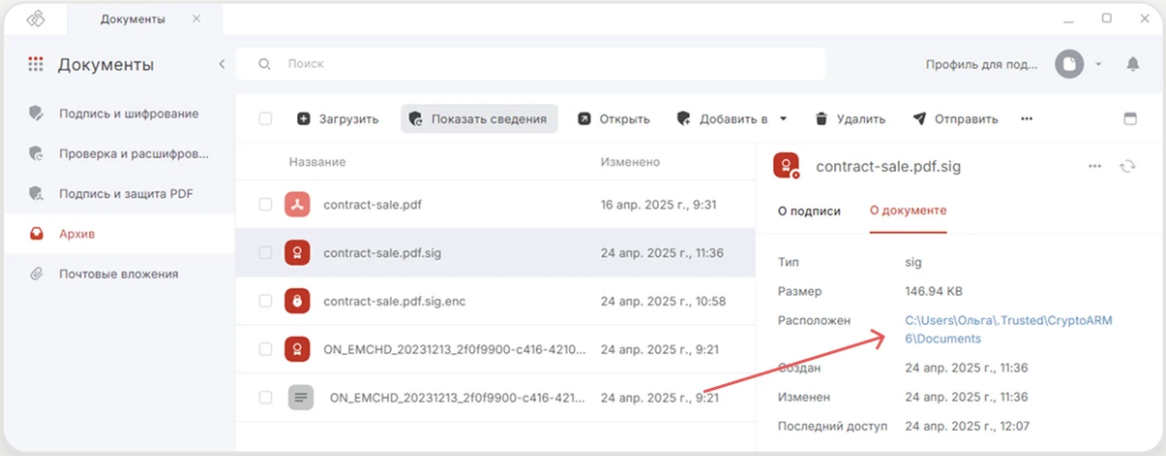
> ⚠️ **Примечание**: Функция доступна только для одиночного выбора документов. При множественном выделении кнопка **Показать в папке** неактивна.

1. Выделите документ в одном из разделов:
    - Папка **Архив**,
    - Мастер **Подпись и шифрование**,
    - Мастер **Проверка и расшифрование**.
2. Нажмите кнопку **Показать в папке** на панели действий.



3. Откроется системная папка с файлом.

> 💡 **Совет**: Также перейти в папку с расположением файла можно при просмотре сведений о файле. Для этого нажмите на путь файла на вкладке **О документе**.



Удаление документа

> ⚠️ **Примечание**: Документы, хранящиеся в папке **Архив**, можно удалить. При этом они будут удалены из файловой системы. Если вы удаляете документы в мастере **Подпись и шифрование** или **Проверка и расшифрование**, список будет очищен, но документы останутся в системе.

Чтобы удалить документ из папки **Архив**:

1. Перейдите в раздел **Документы** → папка **Архив**.
2. Выделите один или несколько документов в списке.

3. Нажмите на кнопку **Удалить** на панели действий.
4. Подтвердите действие в модальном окне.

Инструкции по теме

- Подпись документа со стандартом CAdES
- Подпись документа со стандартом PAdES
- Шифрование документа
- Проверка подписи документа
- Установка личного сертификата

Открыть статью на сайте

Установка личного сертификата

- Перед началом работы
- Установка из ключевого контейнера
- Установка из файла .pfx
- Установка с привязкой к ключевому контейнеру
- Возможные ошибки

Перед началом работы

Перед импортом личного сертификата убедитесь, что:

- установлены корневые сертификаты удостоверяющего центра, который выдал этот сертификат,
- загружен актуальный список отозванных сертификатов (CRL).

Об установке корневых сертификатов читайте в инструкции Установка корневого и промежуточного сертификатов.

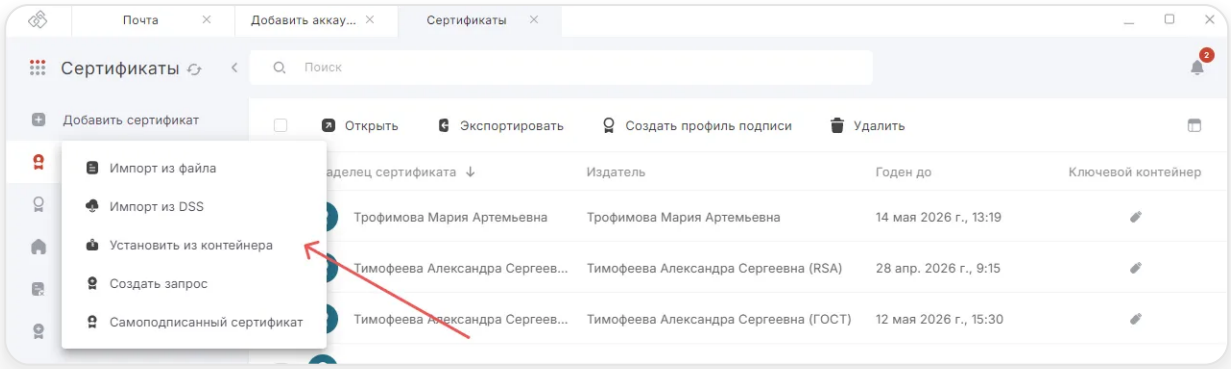
> 💡 **Совет**: Если после установки сертификат не появляется в разделе «Личные сертификаты», обновите список сертификатов с помощью соответствующей кнопки 🔄.

Установка из ключевого контейнера

> 🚨 **Условия**:
>
> - Наличие сертификата в контейнере.
> - Установленные драйверы токена (при необходимости).

Способ 1: Установка из раздела "Сертификаты"

1. При необходимости подключите токен к устройству.
2. Перейдите в раздел **Сертификаты** → **Ключи**.
3. Нажмите кнопку **Добавить сертификат** в боковом меню.
4. В открывшемся списке действий выберите **Установить из контейнера**.

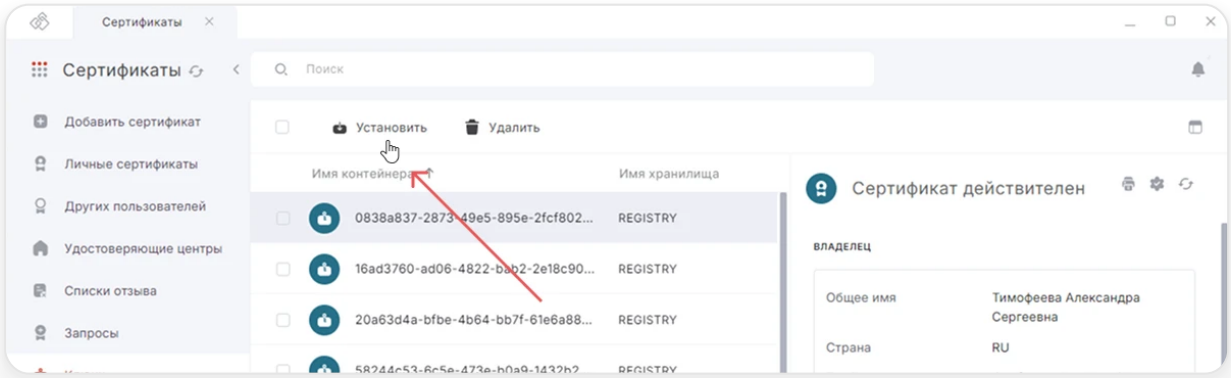


5. Откроется список контейнеров.

6. Выделите необходимый контейнер в списке.

> 💡 **Совет**: С помощью кнопки **Подробно** можно просмотреть сертификат, находящийся в контейнере.

7. Нажмите кнопку **Установить** на панели действий.

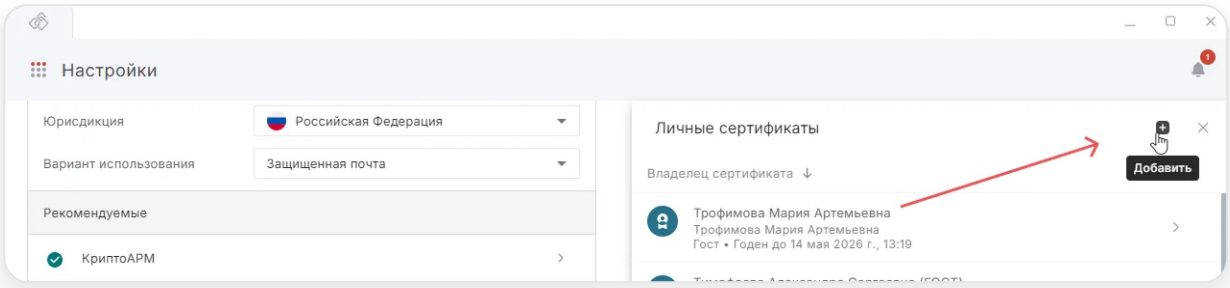


8. При необходимости введите пароль к ключевому контейнеру.

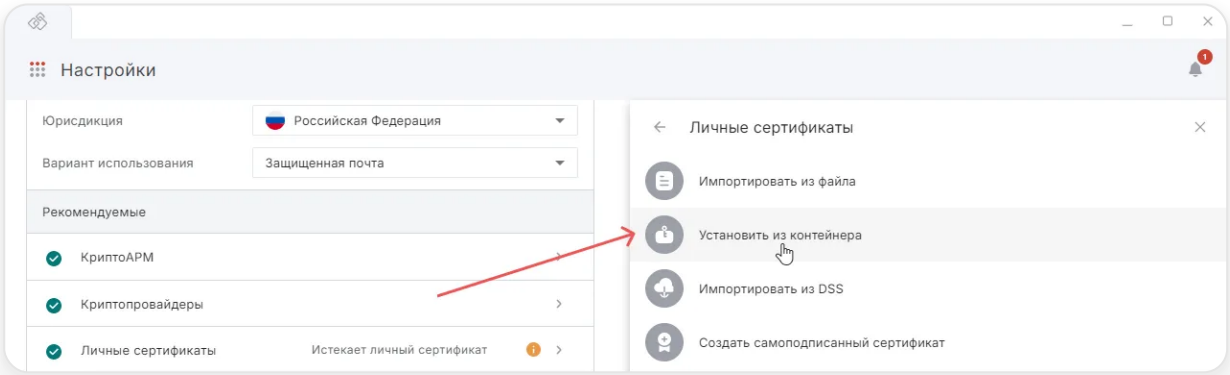
После успешной установки появится уведомление: «Сертификат успешно добавлен в раздел **Личные сертификаты**».

Способ 2: Установка из раздела "Настройки"

1. При необходимости подключите токен к устройству.
2. Перейдите в раздел **Настройки** → проверка **Личные сертификаты**.
3. Откроется окно со списком сертификатов (если они обнаружены).
4. Нажмите на кнопку **Добавить** в верхней части окна.

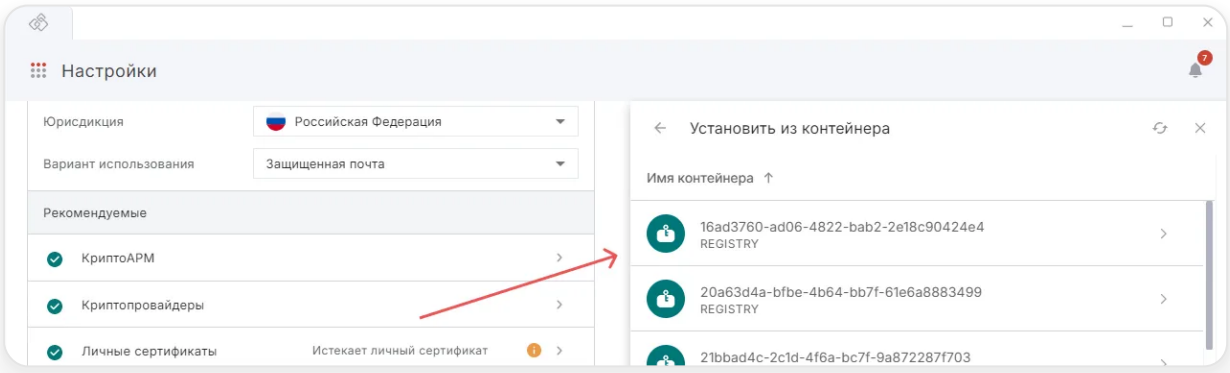


5. Выберите действие **Установить из контейнера**.



6. Откроется список контейнеров.

7. Нажмите на необходимый контейнер в списке.



> 💡 **Совет**: С помощью кнопки **Подробно** > можно просмотреть сертификат, находящийся в контейнере.

8. Нажмите кнопку **Установить** в нижней части окна.

9. При необходимости введите пароль к ключевому контейнеру.

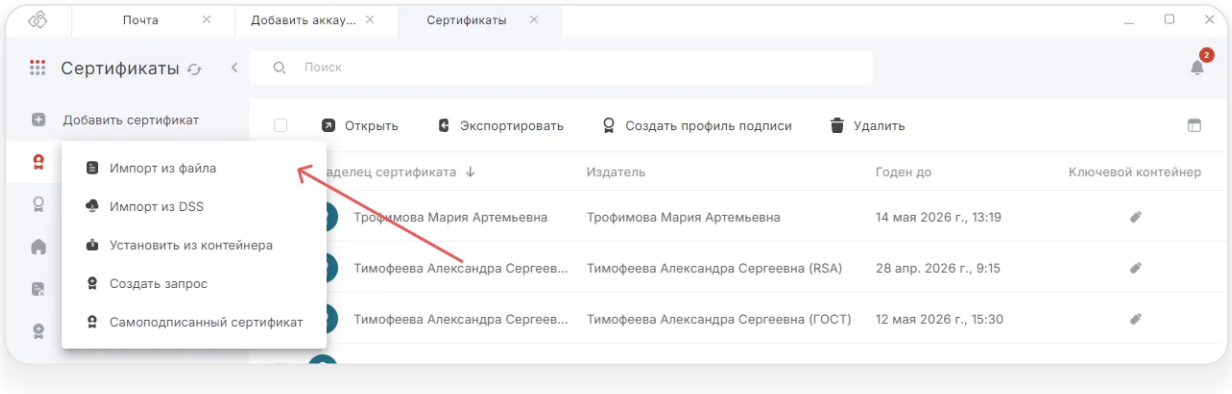
После успешной установки появится уведомление: «Сертификат успешно добавлен в раздел **Личные сертификаты**».

Установка из файла .pfx

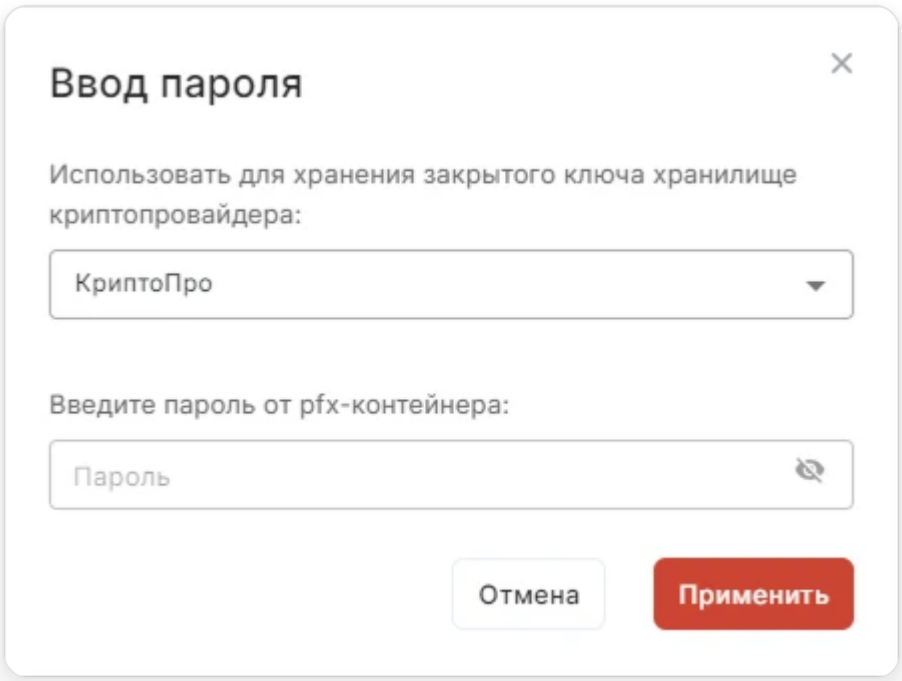
> 💡 Прежде чем приступить к импорту сертификата, убедитесь, что в памяти устройства сохранён файл с расширением `.pfx`, который содержит сертификат.

Способ 1: Установка из раздела "Сертификаты"

1. Перейдите в раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в боковом меню.
3. В появившемся списке действий выберите **Импорт из файла**.



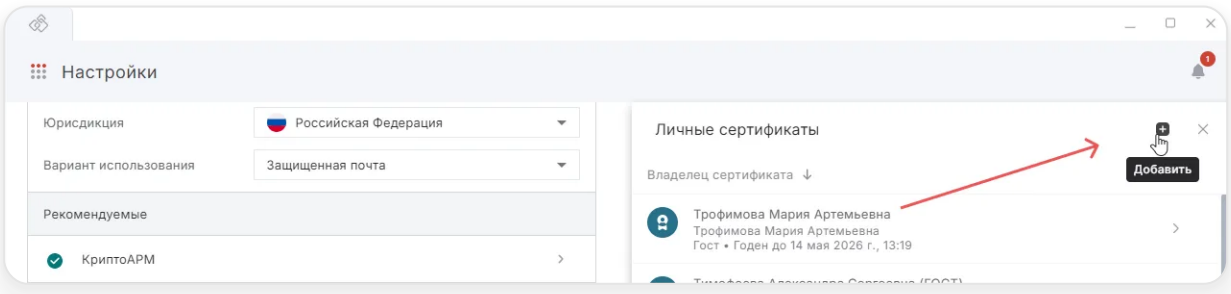
4. В файловом менеджере выберите файл сертификата `.pfx`.
5. В открывшемся окне **Ввод пароля**:
   - Выберите криптопровайдер, в хранилище которого будет установлен сертификат. В текущей версии приложения поддерживаются 2 провайдера: **КриптоПро CSP** и **OpenSSL**.
   - Введите пароль от pfx-контейнера.



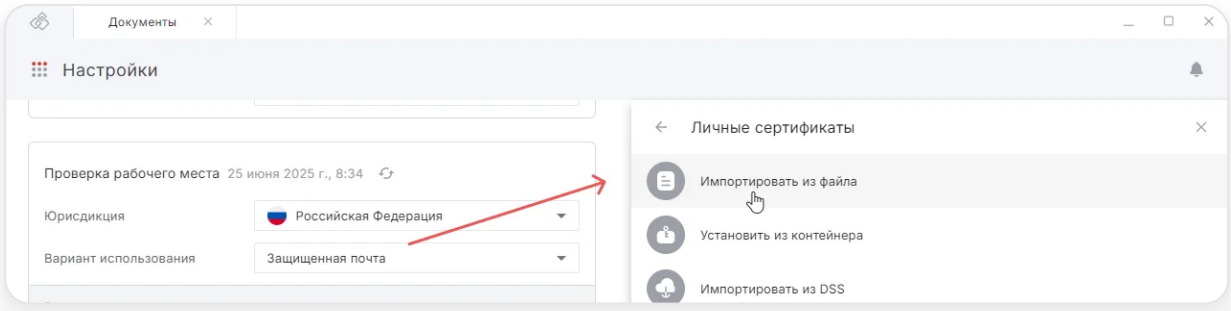
6. При необходимости задайте новый пароль к ключевому контейнеру.

Способ 2: Установка из раздела "Настройки"

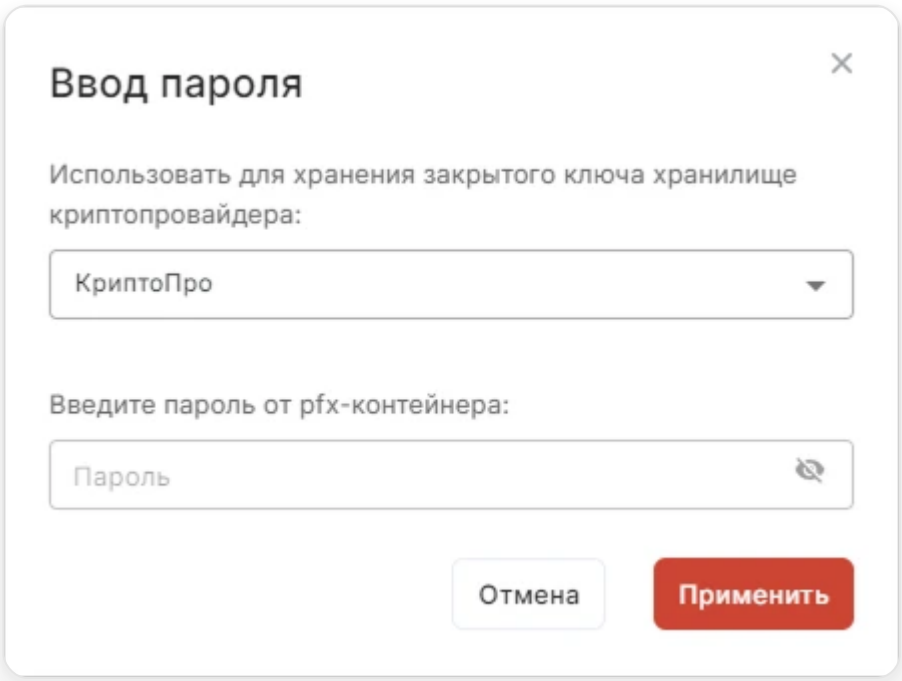
1. Перейдите в раздел **Настройки** → проверка **Личные сертификаты**.
2. Откроется окно со списком сертификатов (если они обнаружены).
3. Нажмите на кнопку **Добавить** в верхней части окна.



4. Выберите действие **Импорт из файла**.



5. В файловом менеджере выберите файл сертификата `.pfx`.
6. В открывшемся окне **Ввод пароля**:
   - Выберите криптопровайдер, в хранилище которого будет установлен сертификат. В текущей версии приложения поддерживаются 2 провайдера: **КриптоПро CSP** и **OpenSSL**.
   - Введите пароль от pfx-контейнера.



7. При необходимости задайте новый пароль к ключевому контейнеру.

Установка с привязкой к ключевому контейнеру

Установка сертификата с привязкой к ключевому контейнеру означает связывание существующего сертификата (без закрытого ключа) с ключевым контейнером, где уже хранится соответствующий закрытый ключ.

1. Перейдите в раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в боковом меню.
3. В появившемся списке действий выберите **Импорт из файла**.
4. В файловом менеджере выберите файл сертификата `.cer` или `.crt`.
5. При необходимости введите пароль к ключевому контейнеру.

Сертификат установлен в хранилище «Личные сертификаты».

Возможные ошибки

При возникновении ошибки вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Описание	Рекомендуемые действия
Не удалось импортировать сертификат. Провайдер с поддержкой ГОСТ алгоритмов не найден.	Отсутствует КриптоПро CSP	Установите криптопровайдер КриптоПро CSP и перезапустите приложение КриптоАРМ
Не удалось импортировать сертификат	При импорте сертификата из файла выбран неподходящий криптопровайдер	Попробуйте импортировать сертификат ещё раз. Выберите другой провайдер.
Не удалось загрузить контейнеры	Отсутствует КриптоПро CSP	Установите криптопровайдер КриптоПро CSP и перезапустите приложение КриптоАРМ

Инструкции по теме

- Установка корневого и промежуточного сертификата
- Импорт списка отзыва сертификатов
- Просмотр уведомлений

Открыть статью на сайте

Установка сертификата из DSS

- Особенности
- Создание подключения к сервису DSS
- Возможные ошибки
- Инструкции по теме

Особенности

Сертификат DSS — сертификат электронной подписи, ключ от которого генерируется и хранится на сервере Удостоверяющего центра. Благодаря этому владельцу сертификата не требуется записывать и хранить ключ на токене или компьютере. Это позволяет ему подписывать электронные документы с любого устройства и из любого места, где есть доступ в интернет.

Подпись документов с помощью сертификата DSS имеет следующие особенности:

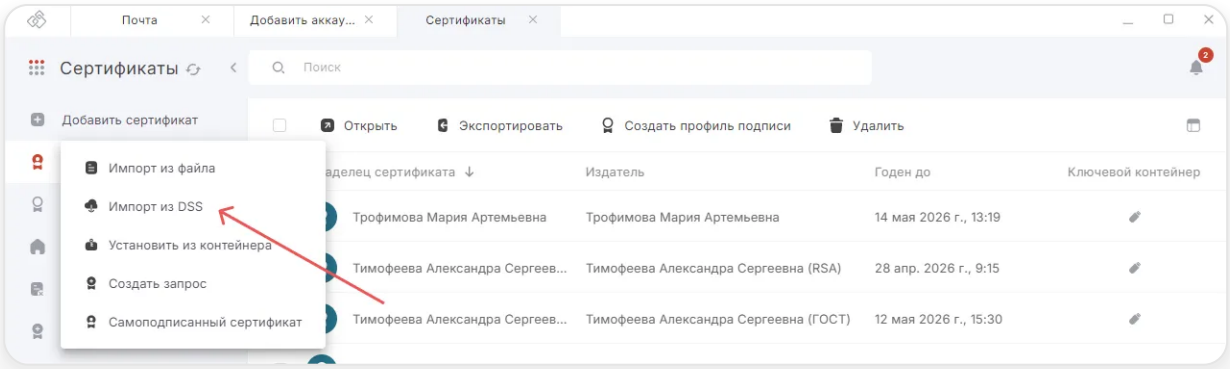
1. **Ограниченные настройки подписи**:
    - Недоступен выбор стандарта подписи PAdES,
    - Отсутствует возможность установки штампов времени.
2. **Процесс аутентификации**:
    - Нужен доступ к интернету,
    - Иногда требуются дополнительные методы подтверждения.

Для установки сертификата из DSS необходимо создать подключение к сервису DSS.

Создание подключения к сервису DSS

Способ 1: Установка из раздела "Сертификаты"

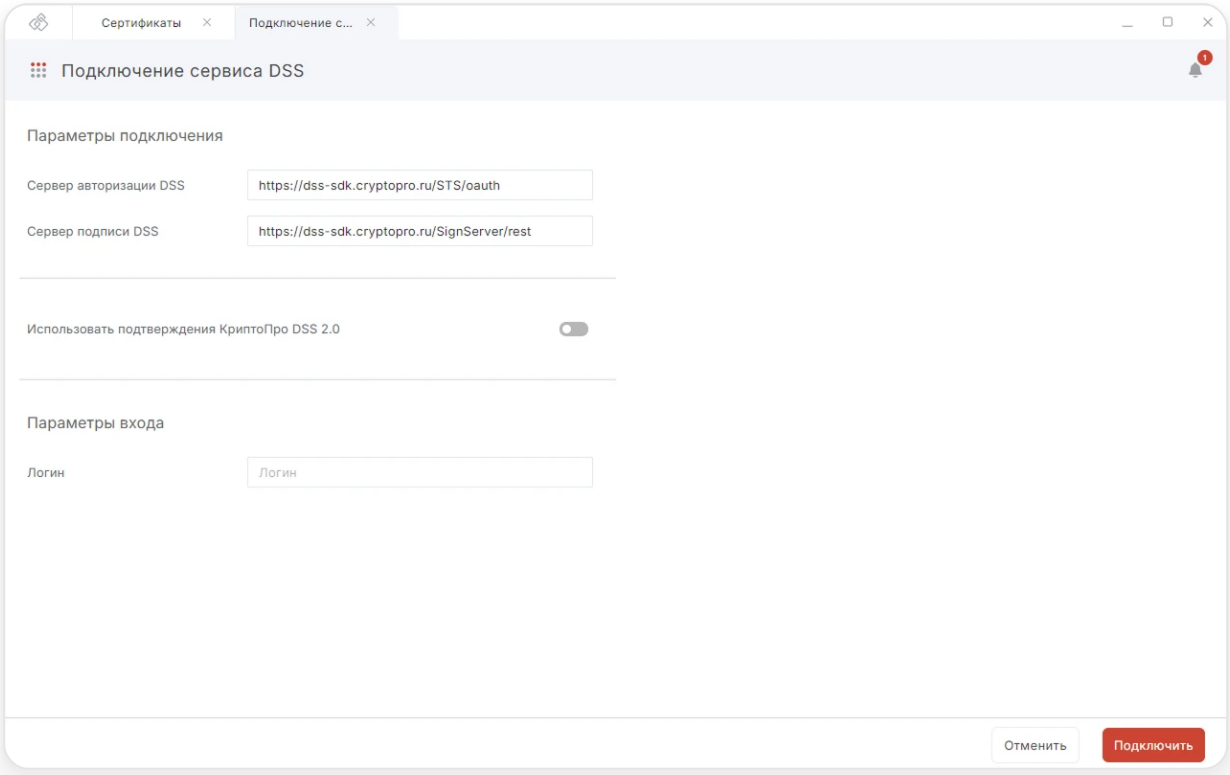
1. Перейдите в раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в боковом меню.
3. В открывшемся списке действий выберите **Импорт из DSS**.



4. Откроется новая вкладка с формой подключения сервиса DSS.

5. Заполните поля:

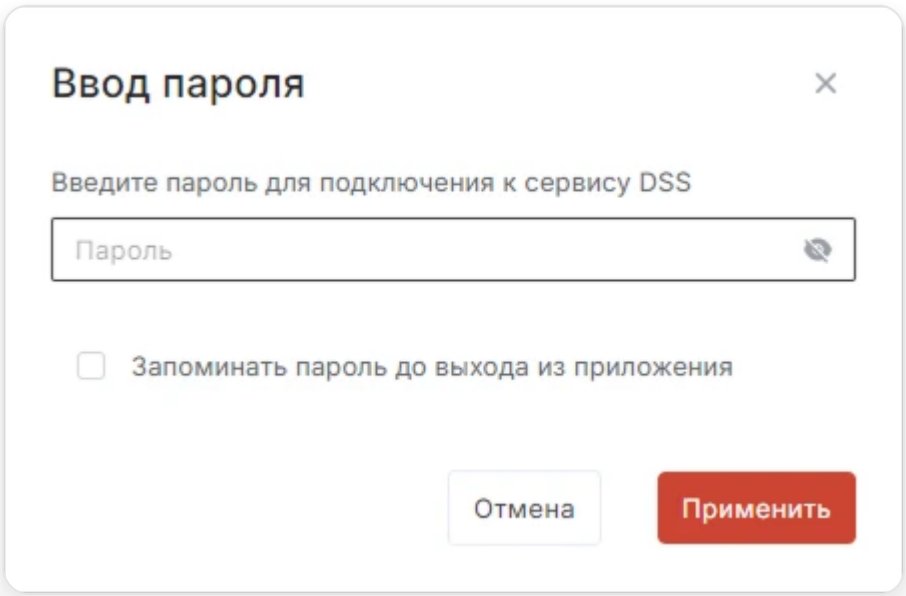
   - **Сервер авторизации DSS** и **Сервер DSS** — данные адреса необходимо получить в организации, предоставившей вам сертификат электронной подписи;
   - **Использовать подтверждения КриптоПро DSS 2.0** — нужно включить данную опцию, если используется продукт КриптоПро DSS 2.0;
   - **Логин** — ваш логин для доступа к сертификату.



6. Нажмите **Подключить**.

7. Если в личном кабинете DSS в настройках стоит подтверждение по паролю, то на следующем шаге введите пароль для подключения к сервису DSS и нажмите кнопку **Применить**.

Чтобы каждый раз не вводить пароль для подключения при работе с сертификатом DSS, можно установить флаг **Запоминать пароль до выхода из приложения**.



Если пароль не задан, то данный шаг пропускается.

8. Если в личном кабинете DSS в настройках стоит подтверждение аутентификации по SIM-карте или с помощью мобильного приложения, то на следующем шаге появляется информационное окно с ожиданием подтверждения операции на телефоне.

   Подтвердите операцию на телефоне.

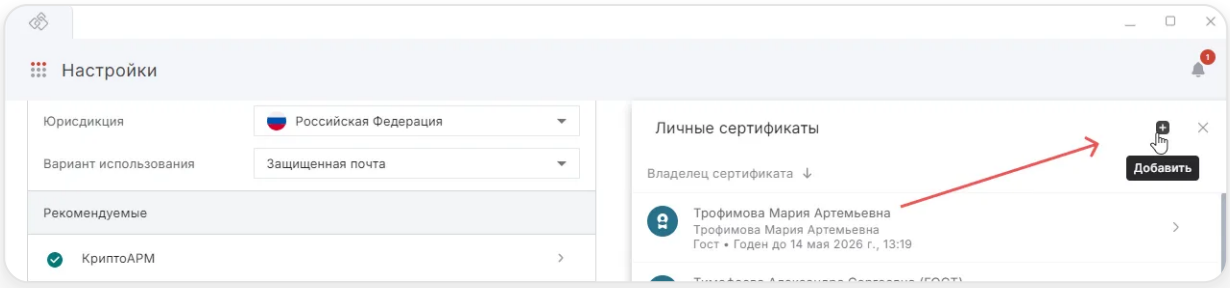
   Если идентификация настроена не с помощью телефона, то данный шаг пропускается.

При успешной аутентификации сертификат DSS автоматически помещается в хранилище **Личные сертификаты**.

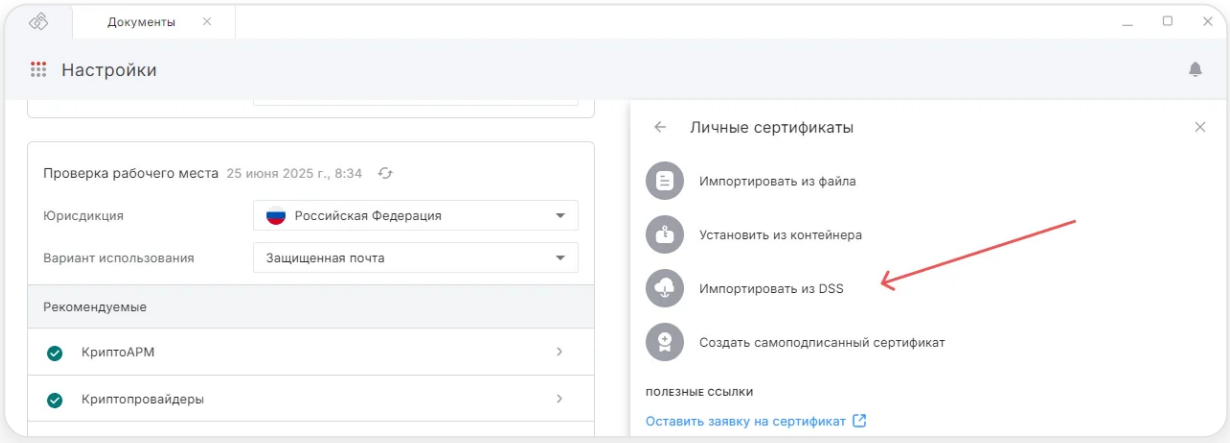
> 💡 Сертификаты DSS в списке отмечаются специальной иконкой .

Способ 2: Установка из раздела "Настройки"

1. Перейдите в раздел **Настройки** → проверка **Личные сертификаты**.
2. Откроется окно со списком сертификатов (если они обнаружены).
3. Нажмите на кнопку **Добавить** в верхней части окна.



4. Выберите действие **Импортировать из DSS**.



5. Откроется новая вкладка с формой подключения сервиса DSS.

6. Следуйте шагам из инструкции Способ 1: Установка из раздела "Сертификаты".

Возможные ошибки

При возникновении ошибки вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Описание	Рекомендуемые действия
Не удалось подключиться к серверу DSS	Возможно, указан неверный логин или пароль	Проверьте правильность заполнения данных
Не удалось подключиться к серверу DSS	Возможно, указаны некорректные адреса серверов, либо отсутствует подключение к сети Интернет	1. Проверьте правильность заполнения данных, 2. Проверьте подключение к сети Интернет.

Инструкции по теме

- Установка корневого и промежуточного сертификатов
- Импорт списка отзыва сертификатов
- Просмотр уведомлений

Открыть статью на сайте

Создание самоподписанного сертификата

- Что такое самоподписанный сертификат?
- Как создать самоподписанный сертификат
- Результаты создания
- Дополнительные действия

Что такое самоподписанный сертификат?

Самоподписанный сертификат — это сертификат электронной подписи, созданный пользователем самостоятельно без обращения в Удостоверяющий центр.

Особенности

- Совмещает функции личного сертификата и корневого сертификата.
- Подходит только для личного или внутреннего использования, например, для тестирования или обмена документами внутри доверенной группы.

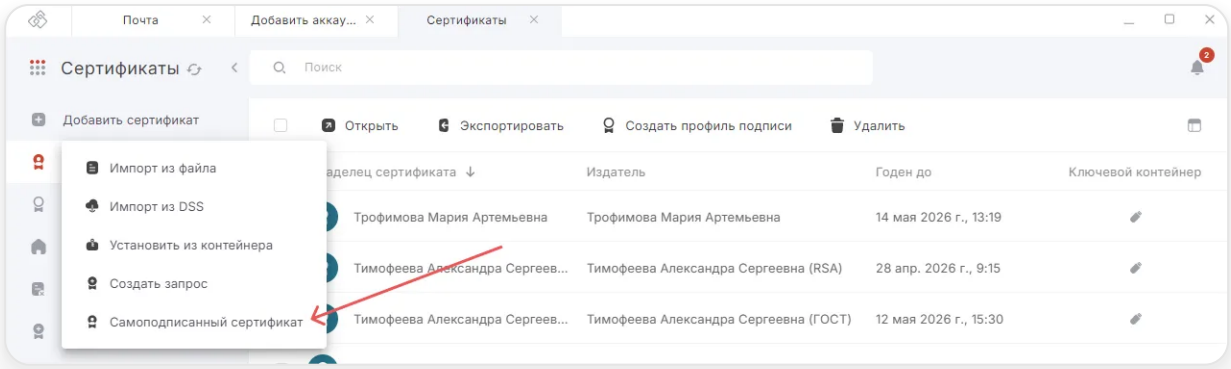
❌ Не подходит для официального документооборота:

- **Нет независимой проверки** — сертификат создан вами, и сторонние организации не могут проверить его подлинность.
- **Нет юридической силы** — государственные порталы, банки и официальные системы требуют сертификаты, выданные доверенными Удостоверяющими центрами.
- **Риск подделки** — любой может создать сертификат с вашим именем, поэтому внешние системы не могут доверять такой подписи автоматически.

Как создать самоподписанный сертификат

Способ 1: Установка из раздела "Сертификаты"

1. Перейдите в раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в боковом меню.
3. В появившемся списке действий выберите **Самоподписанный сертификат**.



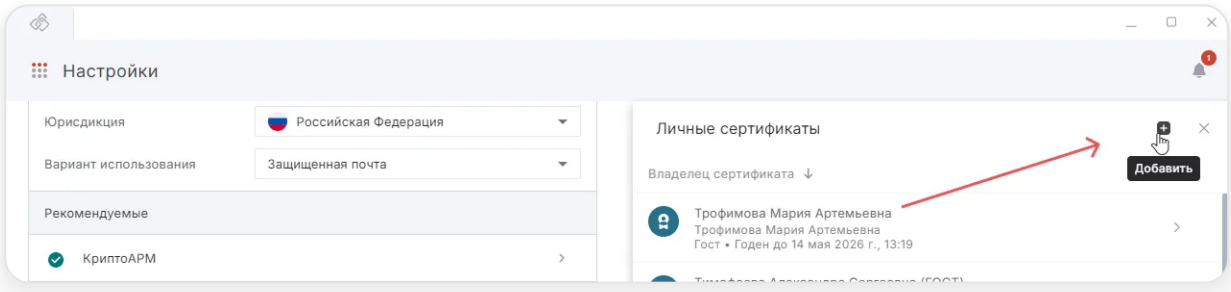
4. Выберите шаблон сертификата.

5. Заполните поля вкладки **Сведения о владельце**. Набор полей меняется в зависимости от выбранного на предыдущем шаге шаблона.
6. Выставите настройки вкладки **Параметры ключа**. Полный список настроек перечислен в разделе Параметры ключа.
7. Нажмите **Сохранить**.
8. При необходимости выберите ключевой носитель для хранения контейнера (реестр, диск, токен).
9. При необходимости установите пароль на контейнер.

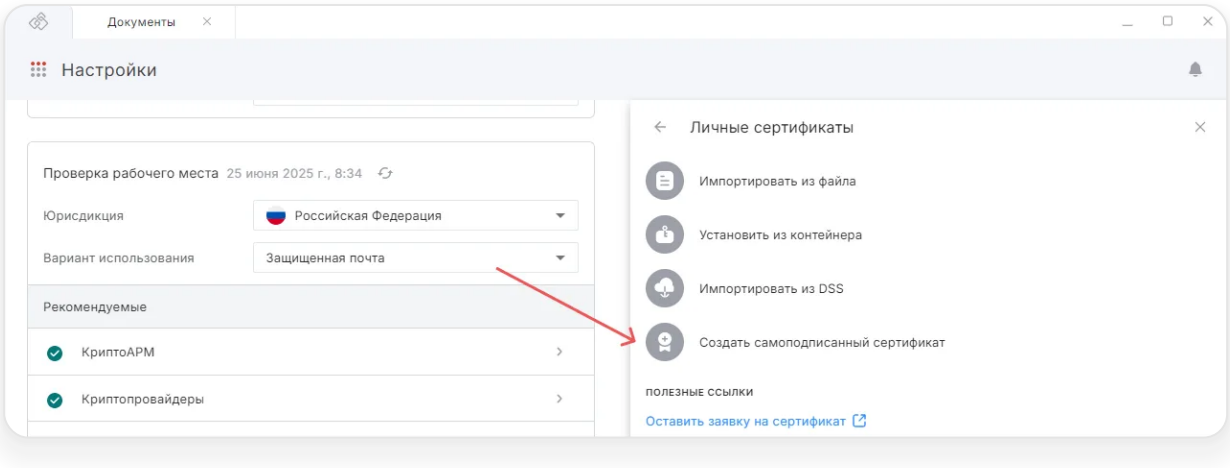
На основе указанных данных формируется самоподписанный сертификат.

Способ 2: Установка из раздела "Настройки"

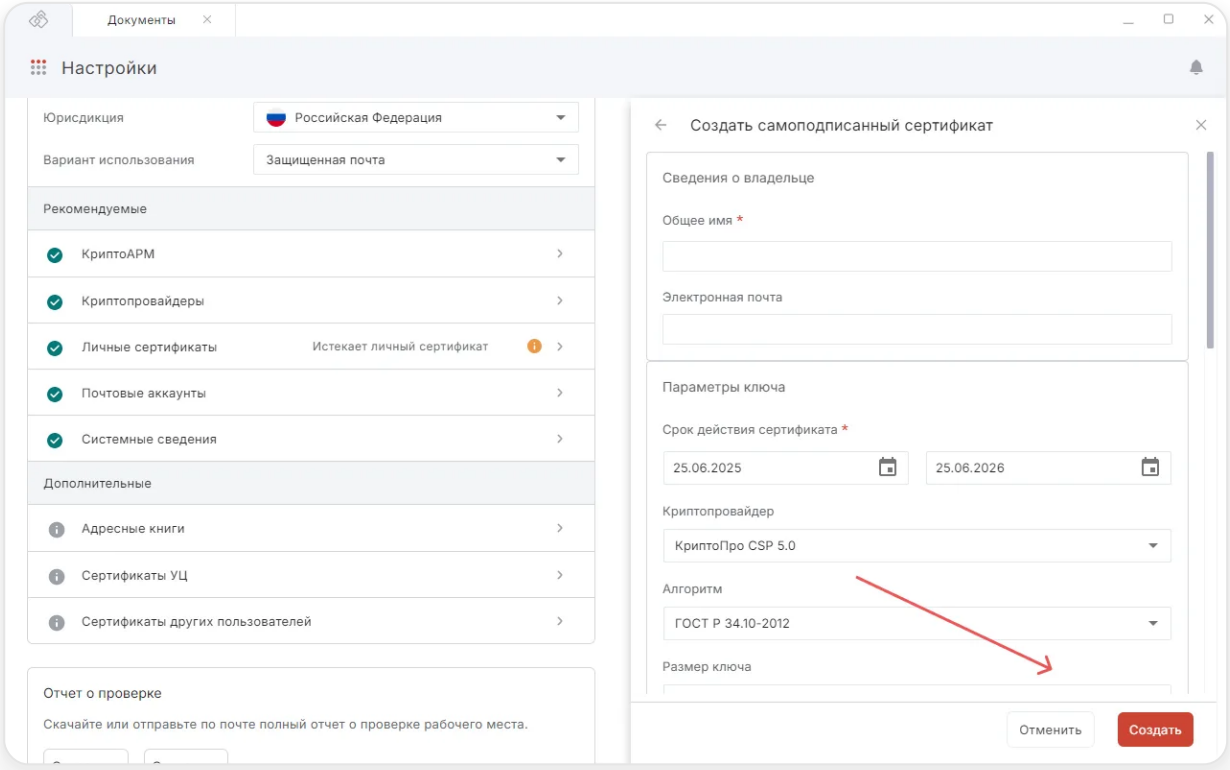
1. Перейдите в раздел **Настройки** → проверка **Личные сертификаты**.
2. Откроется окно со списком сертификатов (если они обнаружены).
3. Нажмите на кнопку **Добавить** в верхней части окна.



4. Выберите действие **Создать самоподписанный сертификат**.



5. В открывшемся окне укажите:
   - Сведения о владельце,
   - Параметры ключа,
   - Использование ключа. Про описание настроек читайте подробнее в инструкции Параметры ключа.



6. Нажмите **Создать**.
7. При необходимости выберите ключевой носитель для хранения контейнера (реестр, диск, токен).
8. При необходимости установите пароль на контейнер.

На основе указанных данных формируется самоподписанный сертификат.

Результаты создания

При успешной генерации сертификат устанавливается в хранилище **Личные сертификаты** раздела **Сертификаты**.

> 💡 **Совет**: Если после создания сертификат не появляется в разделе «Личные сертификаты», обновите список сертификатов с помощью соответствующей кнопки .

Дополнительные действия

Чтобы самоподписанный сертификат был действительным:

1. Экспортируйте сертификат (без закрытого ключа).
2. Импортируйте его в хранилище **Удостоверяющие центры**. Подробнее в инструкции Установка корневого и промежуточного сертификатов.

Инструкции по теме

- Установка корневого и промежуточного сертификатов
- Импорт списка отзыва сертификатов
- Установка личного сертификата
- Создание запроса на сертификат

Открыть статью на сайте

Создание запроса

- Что такое запрос на сертификат?
- Создание запроса на сертификат
- Дальнейшие действия
- Параметры ключа
- Использование ключа

Что такое запрос на сертификат?

Запрос на сертификат — это электронный документ, содержащий необходимые данные для получения сертификата электронной подписи от Удостоверяющего центра (УЦ).

Зачем нужен запрос

Запрос необходим, чтобы УЦ убедился, что создаваемые ключи действительно принадлежат вам, а сведения о владельце верны. Он служит официальным документом для выдачи сертификата.

С помощью запроса можно получить сертификат для:

- Подписи и шифрования документов,
- Обеспечения безопасности электронной почты,
- TLS-сертификатов для сайтов и сервисов.

Шаблоны запросов

В приложении предусмотрены готовые шаблоны запросов, которые помогают быстро и корректно сформировать запрос на сертификат в зависимости от его назначения.

Шаблон	Для кого	Назначение
КЭП ФЛ	Физические лица	Создание запроса на квалифицированный сертификат электронной подписи
КЭП ИП	Индивидуальные предприниматели	Создание запроса на квалифицированный сертификат электронной подписи для индивидуальных предпринимателей
КЭП ЮЛ	Юридические лица	

Шаблон	Для кого	Назначение
		Создание запроса на квалифицированный сертификат электронной подписи сотрудника организации
Расширенный шаблон	ФЛ / ИП / ЮЛ	Создание запроса с расширенным набором атрибутов, когда требуется гибкая настройка данных владельца или специальных параметров сертификата
DV (Domain Validation) — сертификат от Минцифры	ФЛ, ИП, ЮЛ	Создание запроса на сертификат безопасности (TLS). Сертификат подтверждает, что вы управляете доменом, который указан в сертификате, а передача данных пользователей защищена.
OV (Organization Validation) — сертификат от Минцифры	ФЛ, ИП, ЮЛ	Создание запроса на сертификат безопасности (TLS). Сертификат подтверждает, что вы владеете и управляете доменом, который указан в сертификате, а передача данных пользователей защищена.

> 🔍 Подробнее о DV и OV-сертификатах читайте на портале Госуслуги.

Что включает запрос на сертификат

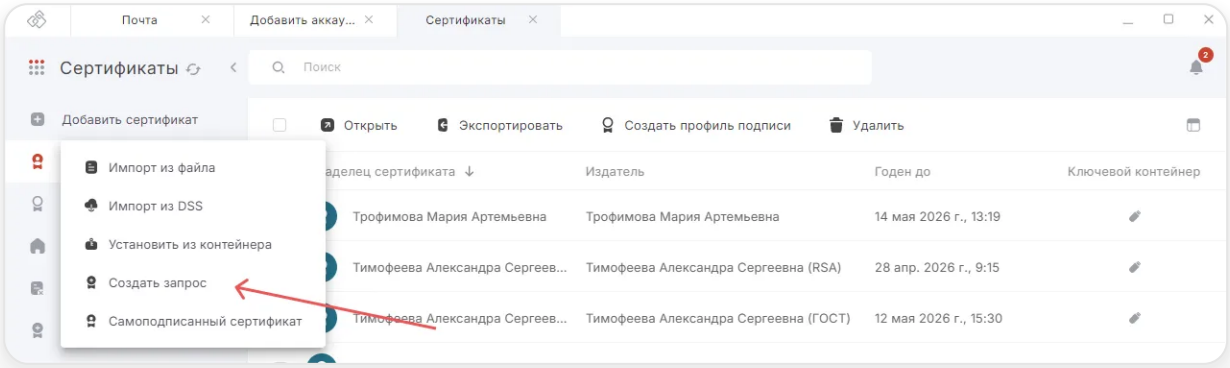
1. **Сведения о владельце**
   - ФИО, должность, организация и контактная информация.
   - Эти данные будут указаны в самом сертификате.
2. **Параметры ключевой пары**
   - Тип и длина ключа,
   - Назначение ключа,
   - Возможность экспорта ключа для переноса на другие устройства.
3. **Технические требования к сертификату**
   - Политики безопасности,
   - Срок действия сертификата,
   - Настройки использования ключа.

Как используется запрос

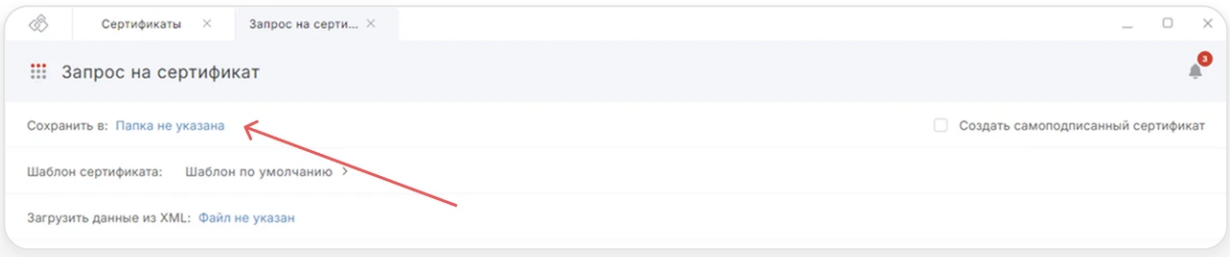
- После создания файла запроса его отправляют в Удостоверяющий центр.
- Удостоверяющий центр проверяет предоставленные данные и создаёт сертификат, который соответствует указанным параметрам.
- После получения сертификата его импортируют в приложение, и он становится готовым для подписания и шифрования документов.

Создание запроса на сертификат

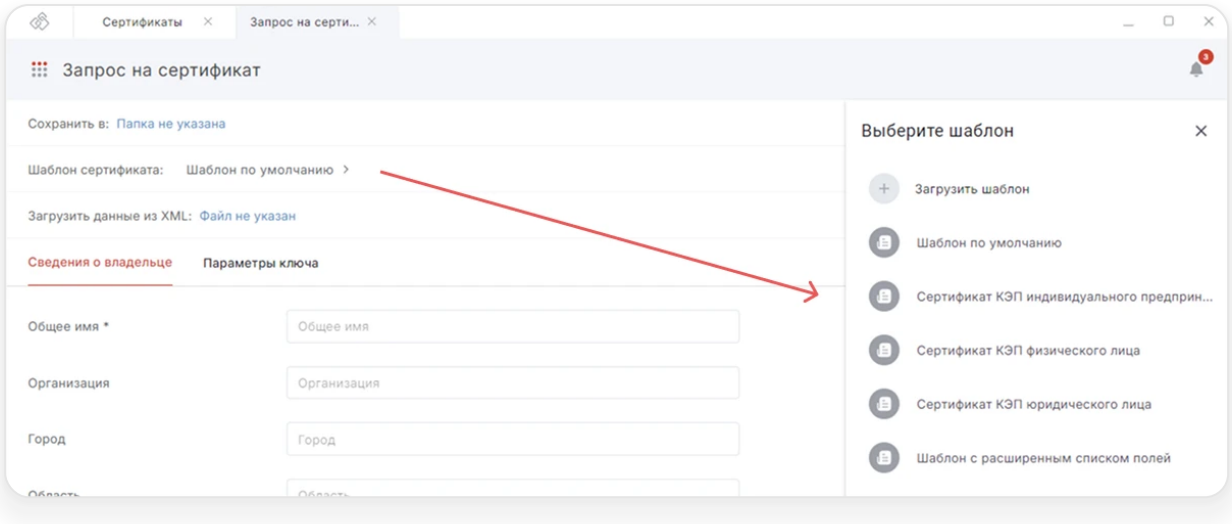
1. Перейдите в раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в боковом меню.
3. В появившемся списке действий выберите **Создать запрос**.



4. Откроется форма создания запроса.
5. В поле **Сохранить в** укажите папку для сохранения файла запроса. Если папка не выбрана, файл запроса сохранится в папку: `C:\Users\Username\.Trusted\CryptoARM 6\Requests`.



6. В поле **Шаблон сертификата** выберите шаблон сертификата. Можно выбрать шаблон из списка или загрузить собственный в формате `.json`.



7. Заполните данные в запросе одним из способов:
    - Загрузите данные из XML — позволяет автоматически заполнить поля в запросе с помощью загрузки файлов XML.
    - Укажите вручную.
8. Заполните поля вкладки **Сведения о владельце**. Набор полей меняется в зависимости от выбранного на предыдущем шаге шаблона.
9. Выставите настройки вкладки **Параметры ключа**. Полный список настроек перечислен в разделе Параметры ключа.
10. Нажмите **Сохранить**.
11. При необходимости выберите ключевой носитель для хранения контейнера (реестр, диск, токен).
12. При необходимости установите пароль на контейнер.

На основе указанных данных сформируется запрос на сертификат.

Дальнейшие действия

После создания запроса на сертификат необходимо отправить его в Удостоверяющий центр для обработки.

> ⚠️ Правила отправки и формат запроса определяются самим УЦ. Перед отправкой уточните эти требования.

Где хранится созданный запрос

После успешного формирования:

- Файл запроса сохраняется в формате: `<CN сертификата>_<алгоритм >_<дата генерации>`.
- Запрос появляется в папке **Запросы** раздела **Сертификаты**.

Импорт готового сертификата

После проверки запроса УЦ выдаст готовый сертификат в виде файла `.cer`.

1. Перейдите в раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в боковом меню.
3. В появившемся списке действий выберите **Импорт из файла**.
4. В файловом менеджере выберите файл сертификата `.cer`.
5. Дождитесь окончания импорта.

После успешного импорта сертификат готов к использованию.

Параметры ключа

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
Криптопровайдер	Выпадающий список	КриптоПро CSP (если установлен)	Криптопровайдер, в хранилище которого будет установлен сертификат	КриптоПро CSP (если установлен), OpenSSL
Алгоритм	Выпадающий список	ГОСТ Р 34.10-2012 или EC	Алгоритм подписи	- ГОСТ Р 34.10-2012, - EC и RSA
Размер ключа	Выпадающий список	512 бит или 384 бит (P-384)	Размер ключа	- Для ГОСТ Р 34.10-2012: 256 бит и 512 бит, - Для EC: 384 бит (P-384), - Для RSA: 2048 бит
Идентификация заявителя	Выпадающий список	-	Процедура проверки личности	- Личное присутствие, - С использование КЭП, - Электронный документ, удостоверяющий личность,

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
				- С использованием сведений ЕСИА и ЕБС
Назначение ключа	Выпадающий список	Подпись и шифрование	Назначение ключа	- Подпись, - Подпись и шифрование, - Шифрование
Контейнер	Поле со значение	Автоматически заданное значение	Название контейнера	-
Пометить ключи как экспортируемые	Переключатель (On/Off)	Off	Если включено, позволяет экспортировать сертификат вместе с закрытым ключом для переноса на другое устройство	On / Off
Средство электронной подписи владельца	Поле для ввода значения	КриптоПро CSP (версия 5.0)	Шифровальное (криптографическое) средство, которое используется для реализации криптографических функций	On / Off
Политики сертификата	Выпадающий список	Класс средства ЭП КС1	Класс средства ЭП зависит от используемого средства подписи и указывает на уровень защиты информации	КС1, КС2, КС3, КВ1, КВ2 и КА

Использование ключа

Указаны значения, выставленные по умолчанию:

Назначение ключа	Подпись	Шифрование	Подпись и шифрование
Подпись (digitalSignature)	✅		✅
Шифрование ключей (keyEncipherment)		✅	✅

Назначение ключа	Подпись	Шифрование	Подпись и шифрование
Неотрекаемость (nonRepudiation/ contentCommitment)	✅		✅
Шифрование данных (dataEncipherment)		✅	✅
Согласование ключей (keyAgreement)	✅	✅	✅
Подпись сертификатов (keyCertSign)			
Подпись CRL (cRLSign)			
Только шифрование (encipherOnly)			
Только расшифрование (decipherOnly)			
Защищенная почта	✅	✅	✅
Проверка подлинности сервера			
Проверка подлинности клиента	✅	✅	✅
Подпись кода			

Инструкции по теме

- Установка корневого и промежуточного сертификатов
- Импорт списка отзыва сертификатов
- Установка личного сертификата
- Создание самоподписанного сертификата

Открыть статью на сайте

Установка корневого и промежуточного сертификатов

- Основные понятия
- Импорт из файла
- Установка при проверке подписи
- Возможные ошибки

Основные понятия

Корневой сертификат — это цифровой документ, в котором содержится информация об удостоверяющем центре. Именно с него начинается «цепочка доверия».

- Корневые сертификаты выпускаются только аккредитованными организациями.
- В России главный корневой сертификат принадлежит **Минцифры РФ**.
- Минцифры подписывает корневым сертификатом сертификаты удостоверяющих центров — они называются **промежуточными**.
- На основе промежуточных сертификатов УЦ выпускает **пользовательские сертификаты** (ваши личные или сертификаты других лиц).

Таким образом, проверка подлинности сертификата всегда строится **снизу вверх**: Пользовательский → Промежуточный → Корневой.

> 🚨 Для корректной проверки статуса сертификата в приложении должны быть установлены **все звенья цепочки доверия** — корневой и все промежуточные сертификаты.

Где взять корневой сертификат

- **На официальном сайте удостоверяющих центров**: обычно в разделе «Поддержка» или «Загрузки» доступны актуальные корневые и промежуточные сертификаты, а также списки отзыва.

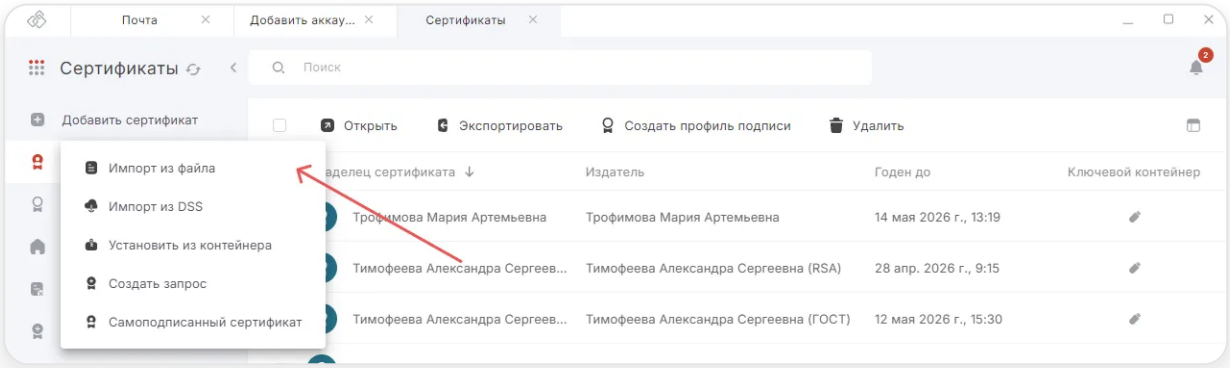
> ⚠️ Всегда скачивайте сертификаты только с официальных сайтов УЦ.

Импорт из файла

> ⚠️ Для установки корневого сертификата могут потребоваться права администратора

Способ 1: Установка из раздела "Сертификаты"

1. Перейдите в раздел **Сертификаты** → **Удостоверяющие центры**.
2. Нажмите кнопку **Добавить сертификат** в боковом меню.
3. В появившемся меню действий выберите **Импорт из файла**.

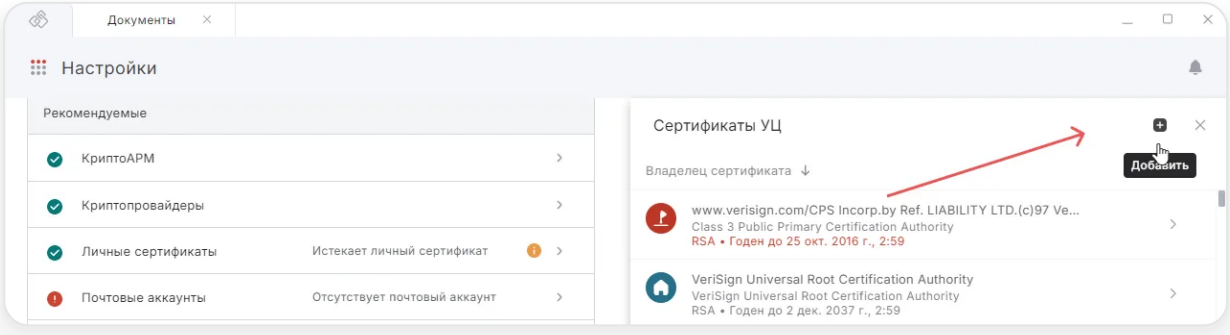


4. В окне файлового менеджера выберите файл сертификата (обычно `.cer` или `.crt`).
5. Подтвердите запрос на установку сертификата.

При успешном импорте сертификат появится в хранилище сертификатов **Удостоверяющие центры**.

Способ 2: Установка из раздела "Настройки"

1. Перейдите в раздел **Настройки** → проверка **Сертификаты других пользователей**.
2. Откроется окно со списком сертификатов (если они обнаружены).
3. Нажмите на кнопку **Добавить** в верхней части окна.

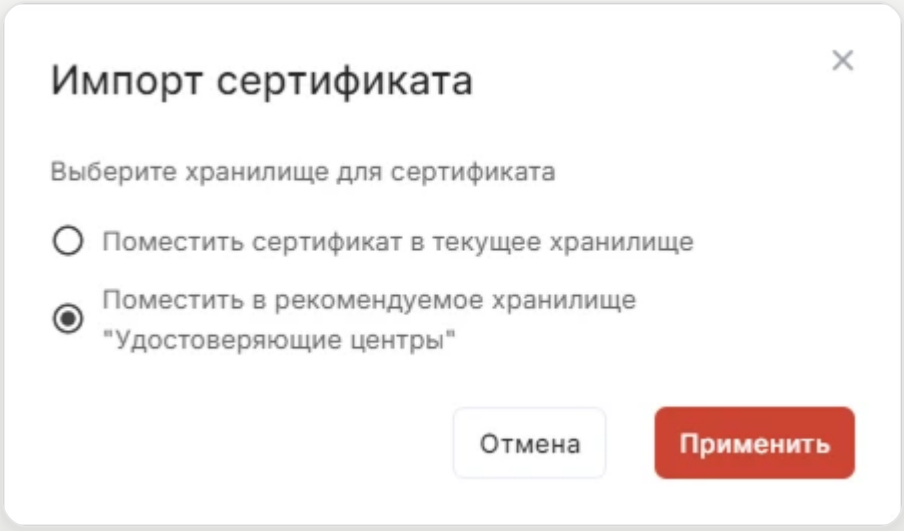


4. Выберите действие **Импортировать из файла**.

5. В окне файлового менеджера выберите файл сертификата (обычно `.cer` или `.crt`).
6. Подтвердите запрос на установку сертификата.

При успешном импорте сертификат появится в хранилище сертификатов **Удостоверяющие центры**.

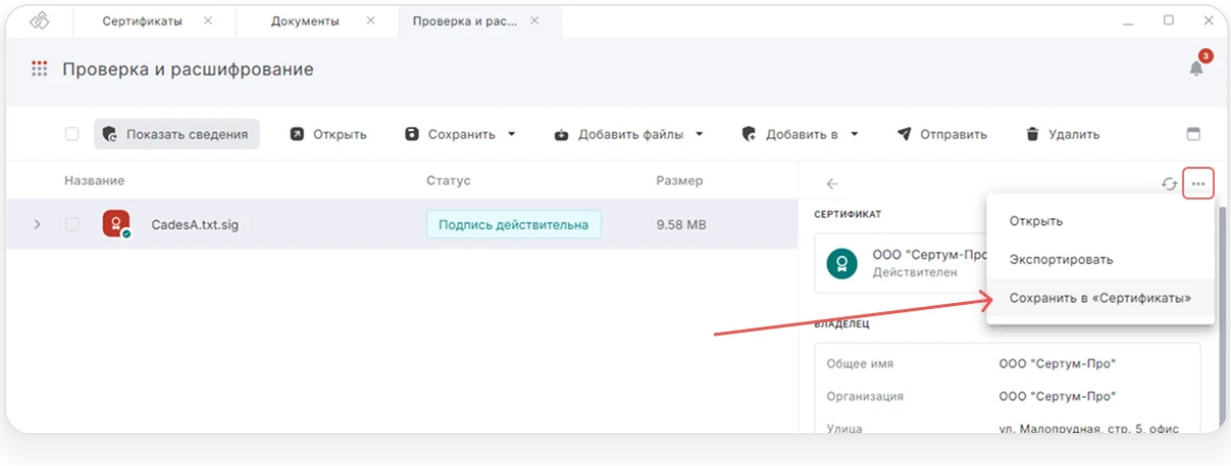
⚠️ **Примечание**: Если выбрано другое хранилище для установки сертификата, КриптоАРМ запросит подтверждение. Для установки сертификата в хранилище «Удостоверяющие центры» выберите опцию «Поместить в рекомендуемое хранилище "Удостоверяющие центры"».



Установка при проверке подписи

1. Выполните проверку подписи документа в мастере **Проверка и расшифрование**. Подробнее в инструкции Проверка подписи документа.
2. Нажмите на кнопку **Показать сведения** или кнопку **Подробно** на панели действий.
3. Справа от списка писем откроется область со сведениями.
4. В блоке **Цепочка сертификации** нажмите на сертификат, который необходимо импортировать.
5. Откроются сведения о сертификате.

6. Вызовите меню действий по кнопке **Еще**.



7. Нажмите на **Сохранить сертификат**.

При успешном импорте сертификат появится в хранилище сертификатов **Удостоверяющие центры**.

Возможные ошибки

При возникновении ошибки вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Описание	Рекомендуемые действия
Не удалось импортировать сертификат	Выбранный сертификат не является корневым или промежуточным сертификатом	1. Проверьте расширение файла (`.cer`, `.crt`) 2. Запросите сертификат повторно у УЦ 3. Убедитесь, что импортируете правильный тип сертификата
Не удалось импортировать сертификат. Провайдер с поддержкой ГОСТ алгоритмов не найден.	Отсутствует КриптоПро CSP	Установите криптопровайдер КриптоПро CSP и перезапустите приложение КриптоАРМ

Инструкции по теме

- Импорт списка отзыва сертификатов
- Установка личного сертификата
- Создание запроса на сертификат
- Создание самоподписанного сертификата

Открыть статью на сайте

Установка сертификатов других пользователей

- Основные понятия
- Импорт из файла
- Установка при проверке подписи документа
- Возможные ошибки

Основные понятия

Для шифрования документов, адресованных другому пользователю, вам потребуется его сертификат.

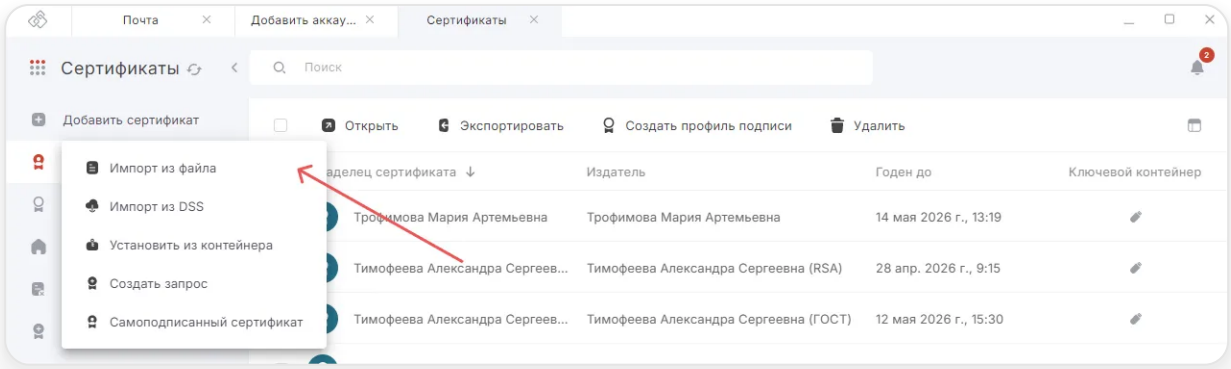
Импорт сертификата, который был отправлен вам другим пользователем, происходит в хранилище сертификатов **Других пользователей**. Он нужен для шифрования документов в адрес этого сертификата. Такой сертификат импортируется без закрытого ключа.

> 🚨 Для того чтобы сертификат был действительным, у вас должны быть установлены корневые и промежуточные сертификаты цепочки сертификации и актуальный список отзыва сертификатов.

Импорт из файла

Способ 1: Установка из раздела "Сертификаты"

1. Перейдите в раздел **Сертификаты** → **Других пользователей**.
2. Нажмите кнопку **Добавить сертификат** в боковом меню.
3. В открывшемся меню действий выберите **Импорт из файла**.

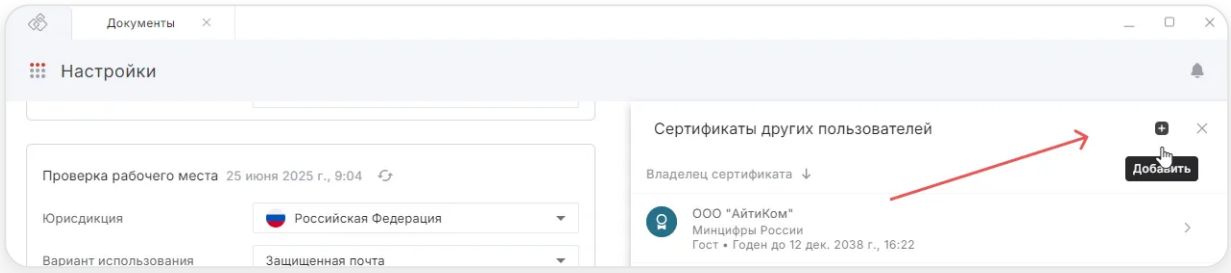


4. В окне файлового менеджера выберите файл сертификата (обычно `.cer` или `.crt`).
5. Подтвердите запрос на установку сертификата.

При успешном импорте сертификат появится в списке хранилища сертификатов **Других пользователей**.

Способ 2: Установка из раздела "Настройки"

1. Перейдите в раздел **Настройки** → проверка **Сертификаты других пользователей**.
2. Откроется окно со списком сертификатов (если они обнаружены).
3. Нажмите на кнопку **Добавить** в верхней части окна.

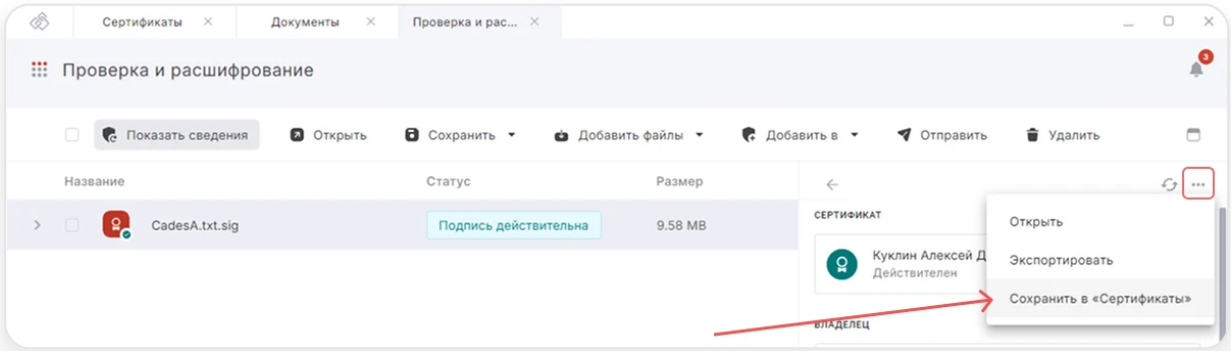


4. Выберите действие **Импортировать из файла**.
5. В открывшемся окне файлового менеджера выберите файл сертификата (обычно `.cer` или `.crt`).
6. Подтвердите запрос на установку сертификата.

При успешном импорте сертификат появится в списке хранилища сертификатов **Других пользователей**.

Установка при проверке подписи документа

1. Выполните проверку подписи документа в мастере **Проверка и расшифрование**. Подробнее в инструкции Проверка подписи документа.
2. Нажмите на кнопку **Показать сведения** или кнопку **Подробно** на панели действий.
3. Справа от списка откроется область со сведениями.
4. В блоке **Цепочка сертификации** нажмите на сертификат подписанта.
5. Откроются сведения о сертификате.
6. Вызовите меню действий по кнопке **Еще**.

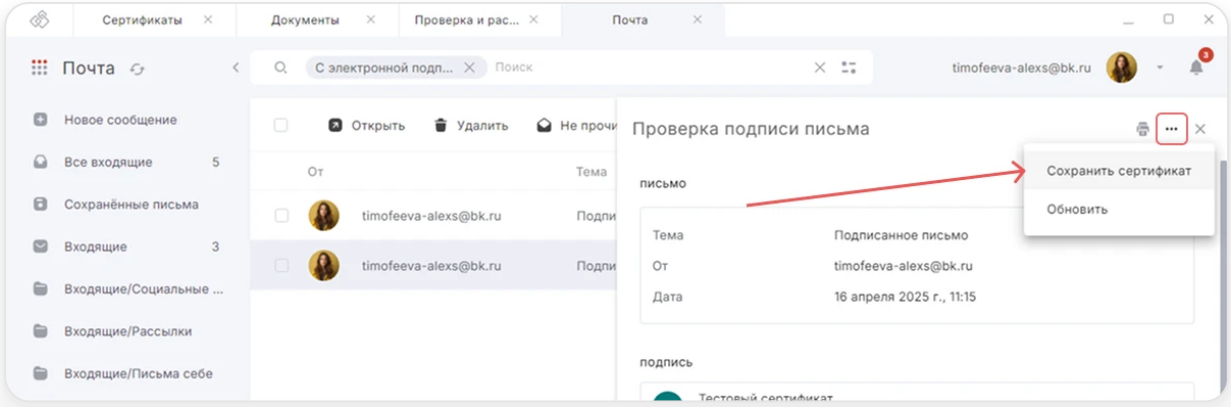


7. Нажмите на **Сохранить сертификат**.

Сертификат будет успешно сохранен в хранилище сертификаты «Других пользователей».

Способ 3: Установка при проверке подписи письма

1. Откройте сведения о подписи письма. Подробнее в инструкции Как проверить подпись письма.
2. Вызовите меню действий по кнопке **Еще**.



3. Нажмите на **Сохранить сертификат**.

Сертификат будет успешно сохранен в хранилище сертификаты «Других пользователей».

Возможные ошибки

При возникновении ошибки вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Описание	Рекомендуемые действия
Не удалось импортировать сертификат. Провайдер с поддержкой ГОСТ алгоритмов не найден.	Отсутствует КриптоПро CSP	Установите криптопровайдер КриптоПро CSP и перезапустите приложение КриптоАРМ
Не удалось импортировать сертификат	Возможно, выбрано не подходящее хранилище для сертификата	Перейдите в раздел **Сертификаты → Других пользователей** и повторите попытку установки.

Инструкции по теме

- Импорт списка отзыва сертификатов
- Установка личного сертификата
- Создание запроса на сертификат
- Создание самоподписанного сертификата

Открыть статью на сайте

Установка списка отзыва

- Основные понятия
- Установка списка отзыва

Основные понятия

Список отзыва сертификатов (COC) или **Certificate Revocation List** (CRL) — это специальный цифровой документ, публикуемый удостоверяющим центром. В нём содержатся сведения о сертификатах, которые были признаны недействительными до окончания срока их действия.

Использование COC необходимо для проверки актуальности сертификатов и исключения компрометированных ключей из доверенной среды.

Основные причины отзыва:

- Компрометация закрытого ключа (потеря, кража токена)
- Изменение данных владельца (смена фамилии, реквизитов организации)
- Ошибки при выпуске сертификата
- Прекращение деятельности удостоверяющего центра
- Нарушение условий использования

> 📌 **Проверка COC** — обязательная часть процесса подтверждения подлинности сертификатов. Если сертификат присутствует в списке отзыва, его использование считается недопустимым.

Где взять список отзыва

Списки отзыва публикуются удостоверяющими центрами, которые выпускают сертификаты.

Получить списки отзыва можно несколькими способами:

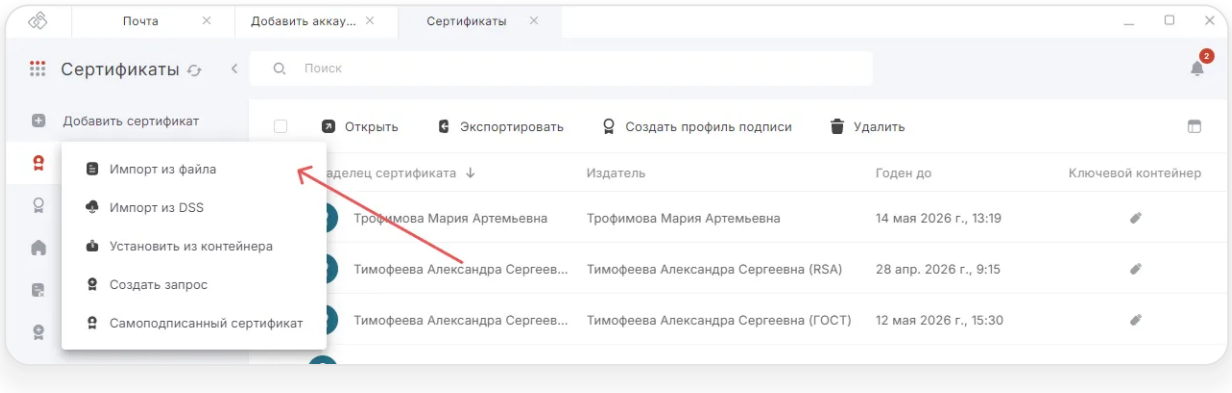
1. **На официальном сайте удостоверяющих центров**: обычно в разделе «Поддержка» или «Загрузки» доступны актуальные версии COC вместе с корневыми и промежуточными сертификатами.
2. **Из личного сертификата**: в свойствах сертификата есть поле **CRL Distribution Point (CDP)**. По указанной там ссылке (`http://...`) можно скачать актуальный COC.

> ⚠️ Списки отзыва имеют ограниченный срок действия. По его истечении необходимо скачать и установить обновлённую версию.

⚠️ Всегда скачивайте списки отзыва только с официальных сайтов УЦ.

Как установить список отзыва

1. Перейдите в раздел **Сертификаты** → **Списки отзыва**.
2. Нажмите кнопку **Добавить сертификат** в боковом меню.
3. В открывшемся меню действий выберите **Импорт из файла**.



4. В окне файлового менеджера выберите файл списка отзыва (обычно `.crl`).
5. Подтвердите запрос на установку списка.

При успешном импорте СОС отображается в разделе **Списки отзыва**.

Инструкции по теме

- Установка корневого и промежуточного сертификатов
- Установка личного сертификата
- Создание самоподписанного сертификата

Открыть статью на сайте

Экспорт личного сертификата

- Основные принципы экспорта
- Экспорт без закрытого ключа
- Экспорт с закрытым ключом
- Инструкции по теме

Основные принципы экспорта

Экспорт сертификата — это сохранение его в файл для дальнейшего использования или передачи другим пользователям.

Для безопасного обмена зашифрованными данными необходимо правильно экспортировать сертификаты.

Существует два основных варианта экспорта:

1. **Без закрытого ключа** — стандартный и безопасный способ.
    - Используется для передачи сертификата коллегам, партнёрам или сервисам.
    - Получатели смогут зашифровать данные для вас или проверить вашу подпись.
    - При этом ваш закрытый ключ остаётся в безопасности.
2. **С закрытым ключом** — используется только в особых случаях.
    - Позволяет перенести сертификат на другое устройство или создать резервную копию.
    - Хранение и передача таких файлов требует строгой защиты.

> ⚠️ **Важно**: экспорт с закрытым ключом доступен только если при создании сертификата был установлен флаг «Экспортируемый». Если он не был задан, выполнить экспорт ключа невозможно.

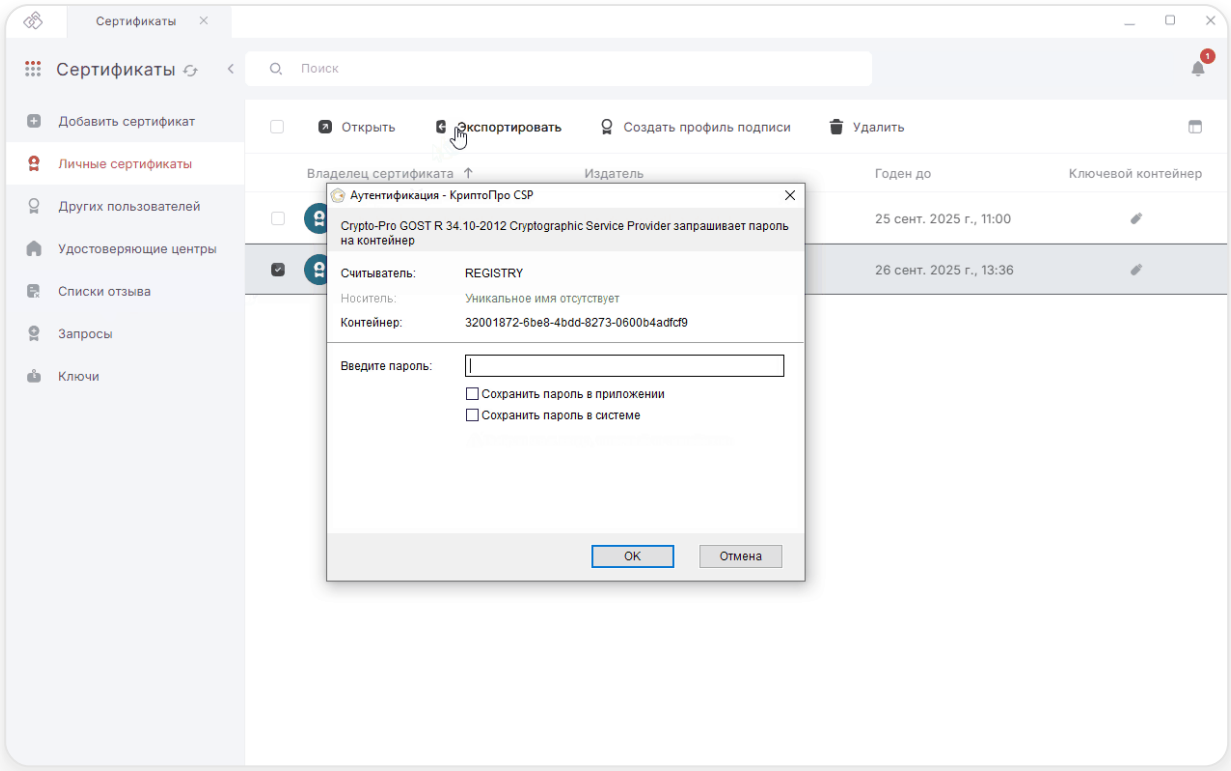
Сравнение способов экспорта

Параметр	Без закрытого ключа	С закрытым ключом
Назначение	Передача сертификата другим людям или системам	Перенос сертификата на другое устройство, резервное копирование
Можно использовать для	Проверки подписи, шифрования данных для вас	Подписи и расшифровки на другом устройстве

Параметр	Без закрытого ключа	С закрытым ключом
Безопасность	Безопасно, т.к. закрытый ключ остаётся у вас	Опасно при неправильном хранении: возможна компрометация ключа
Кому можно передавать	Любому получателю, кому нужно знать ваш открытый ключ	Только самому себе (для переноса) или доверенным лицам под вашу ответственность
Формат файла	`.cer`	`.pfx` (пароль обязателен)

Экспорт без закрытого ключа

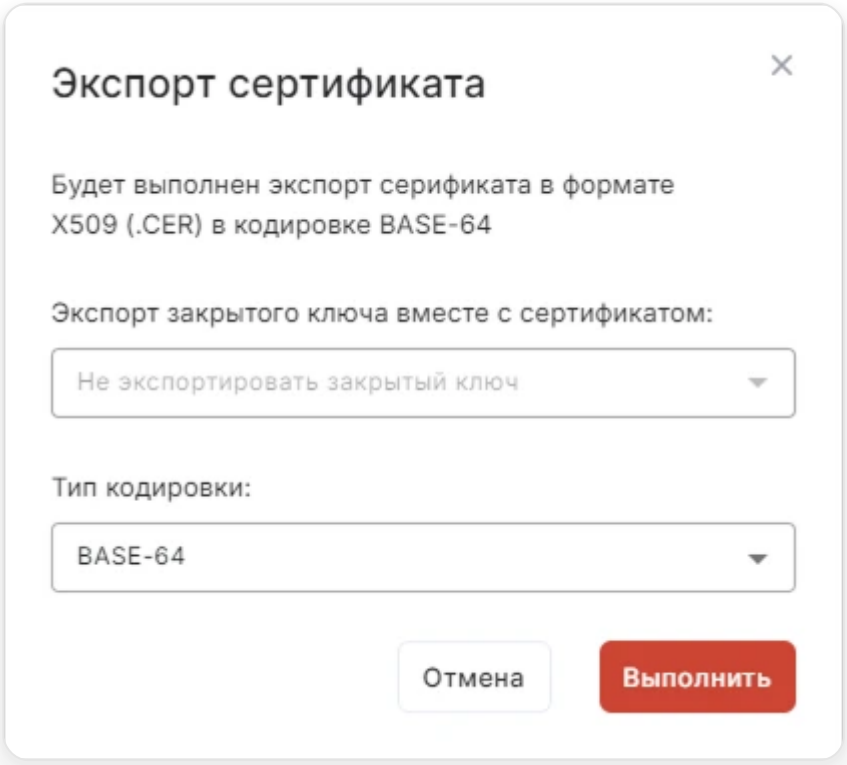
1. Перейдите раздел **Сертификаты** → **Личные сертификаты**.
2. Выделите личный сертификат в списке.
3. Нажмите кнопку **Экспортировать** на панели действий.
4. При необходимости введите пароль к ключевому контейнеру.
5. Откроется окно **Экспорт сертификата**.
    - Выберите **Не экспортировать закрытый ключ**. Выбор может быть заблокирован, если ключ не экспортируемый.
    - Выберите тип кодировки `BASE64` или `DER`.
6. Нажмите кнопку **Выполнить**.
7. В файловом менеджере задайте путь к файлу сертификата и имя файла.



Статичный кадр демонстрации. Открыть анимацию

Экспорт с закрытым ключом

1. Перейдите раздел **Сертификаты** → **Личные сертификаты**.
2. Выделите личный сертификат в списке.
3. Нажмите кнопку **Экспортировать** на панели действий.
4. При необходимости введите пароль к ключевому контейнеру.
5. Откроется окно **Экспорт сертификата**.
    - Выберите **Экспортировать закрытый ключ**. Выбор экспорта закрытого ключа может быть заблокирован, если ключ не экспортируемый.
    - Выберите тип кодировки `BASE64` или `DER`.



6. Укажите пароль от PFX-контейнера.
7. Нажмите кнопку **Выполнить**.
8. В файловом менеджере задайте путь к файлу сертификата и имя файла.

При успешном выполнении операции сертификат экспортируется в файл.

Инструкции по теме

- Экспорт сертификата
- Установка личного сертификата
- Импорт сертификатов других пользователей

Открыть статью на сайте

Экспорт сертификата

- Зачем нужны сертификаты других пользователей
- Способ 1: Стандартный способ
- Способ 2: Экспорт при проверке подписи документа
- Инструкции по теме

Зачем нужны сертификаты других пользователей

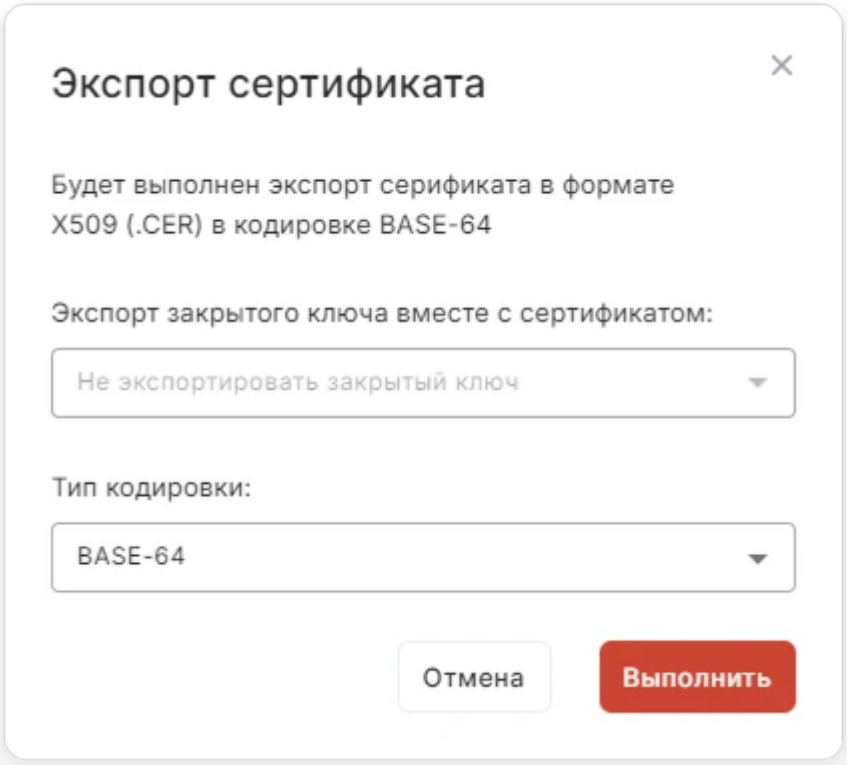
Сертификаты других пользователей нужны для безопасного обмена зашифрованными документами.

Когда вы хотите переслать коллеге или партнёру конфиденциальную информацию (например, договор, отчёт или персональные данные), документ шифруется с использованием открытого ключа получателя, который хранится в его сертификате.

> 💡 **Совет**: Чтобы упростить работу, привяжите сертификат к контакту пользователя — это ускорит поиск и исключит ошибки при выборе сертификата.
>
> ⚠️ **Примечание**: Сертификаты других пользователей, корневые и промежуточные сертификаты экспортируются без закрытого ключа.

Способ 1: Стандартный способ

1. Перейдите в раздел **Сертификаты** и выберите хранилище **Удостоверяющие центры** или **Других пользователей**.
2. Выделите сертификат в списке.
3. Нажмите кнопку **Экспортировать** на панели действий.
4. Откроется окно **Экспорт сертификата**.



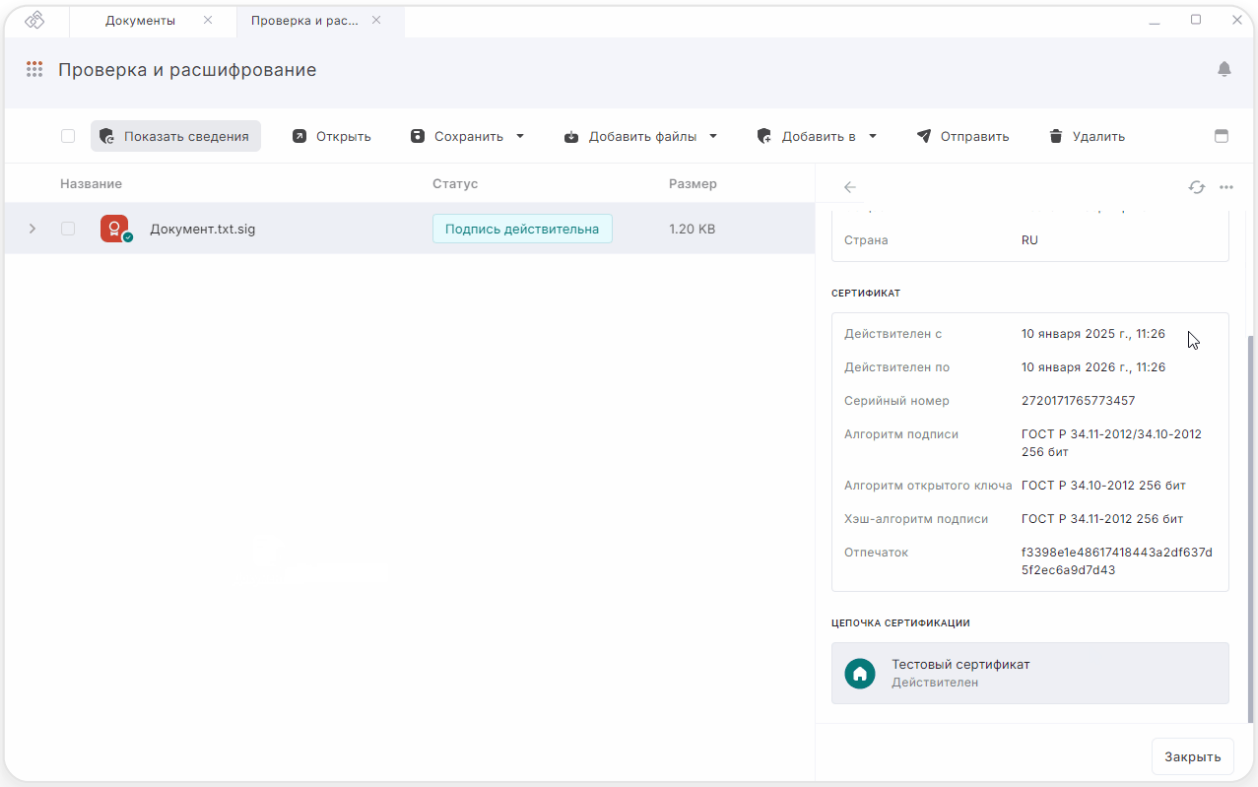
5. Выберите тип кодировки **BASE64** или **DER**.
6. Нажмите кнопку **Выполнить**.
7. В файловом менеджере задайте путь к файлу сертификата и имя файла.

При успешном выполнении операции сертификат экспортируется в файл.

Способ 2: Экспорт при проверке подписи документа

1. Выполните проверку подписи документа в мастере **Проверка и расшифрование**. Подробнее в инструкции Проверка подписи документа.
2. Нажмите на кнопку **Показать сведения** или кнопку **Подробно** на панели действий.
3. Справа от списка откроется область со сведениями.
4. В блоке **Цепочка сертификации** нажмите на сертификат подписанта.
5. Откроются сведения о сертификате.
6. Вызовите меню действий по кнопке **Еще**.
7. Нажмите на **Экспортировать**.
8. Откроется окно **Экспорт сертификата**.
9. Укажите параметры экспорт и нажмите **Выполнить**.
10. Укажите путь для сохранения файла с сертификатом в окне файлового менеджера.

При успешном выполнении операции сертификат экспортируется в файл.



Статичный кадр демонстрации. Открыть анимацию

Инструкции по теме

- Просмотр уведомлений
- Экспорт личного сертификата
- Импорт сертификатов других пользователей

Открыть статью на сайте

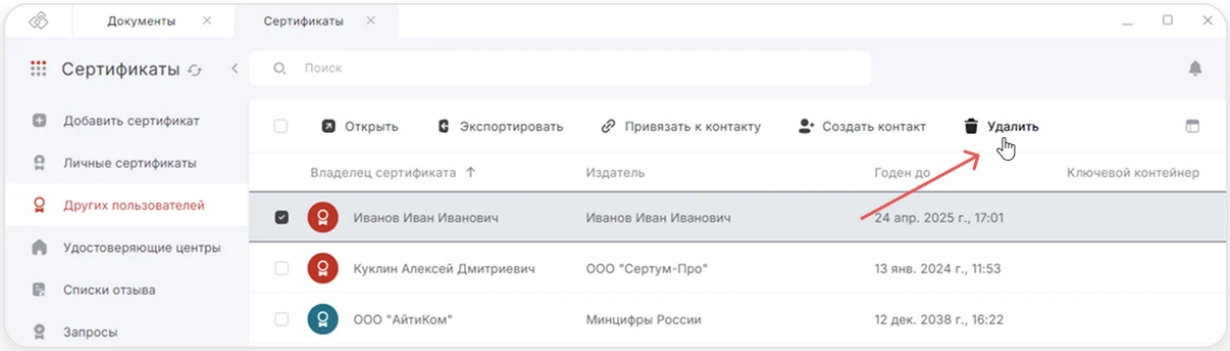
Удаление сертификата

Чтобы удалить сертификат:

1. Перейдите в раздел **Сертификаты**.
2. Выберите хранилище, из которого необходимо удалить сертификат.
3. Выделите сертификат в списке.
4. Нажмите кнопку **Удалить**.

> ⚠️ **Примечание**: если у сертификата есть привязка к закрытому ключу, то при удалении сертификата возможно удаление закрытого ключа. Для этого в окне подтверждения удаления установите флаг **Удалить связанный с сертификатом контейнер**.
>
> 💡 **Совет**: Не рекомендуется удалять контейнер закрытого ключа, так как он не подлежит восстановлению.

5. Подтвердите удаление.



Сертификат будет успешно удален из хранилища.

Инструкции по теме

- Установка корневого и промежуточного сертификатов
- Экспорт личного сертификата
- Импорт сертификатов других пользователей

Открыть статью на сайте

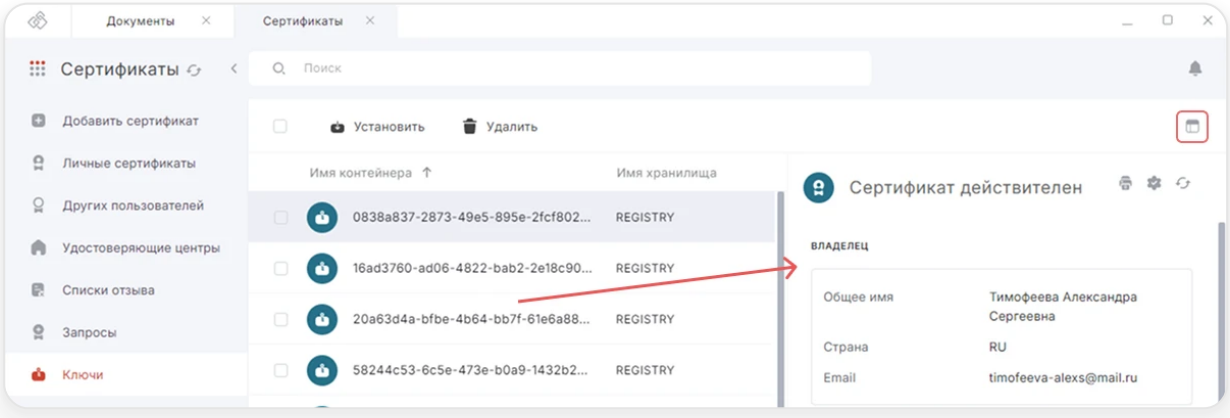
Действия с ключевыми контейнерами

- Просмотр сведений о сертификате
- Печать сведений о сертификате
- Проверка наличия закрытого ключа
- Удаление контейнера
- Обновление списка контейнеров
- Возможные ошибки

> 💡 **Совет**: В программе отображаются ключевые контейнеры, расположенные в системе и на отчуждаемых носителях, например, USB-токенах и смарт-картах.

Просмотр сведений о сертификате

1. При необходимости подключите ключевой носитель к устройству.
2. Перейдите в раздел **Сертификаты** → **Ключи**.
3. Выделите контейнер в списке.
4. Нажмите на кнопку **Подробно** на панели действий.



5. Справа от списка откроется область со сведениями. Если появляется сообщение «В контейнере нет сертификатов», это означает, что контейнер не содержит сертификатов.

Печать сведений о сертификате

> ⚠ **Примечание**: Данная функция доступна только для контейнеров, в которых есть сертификат.

1. При необходимости подключите ключевой носитель к устройству.
2. Перейдите в раздел **Сертификаты** → **Ключи**.
3. Выделите контейнер в списке.
4. Нажмите на кнопку **Подробно** на панели действий.
5. Справа от списка откроется область со сведениями.
6. Нажмите на кнопку **Печать** .

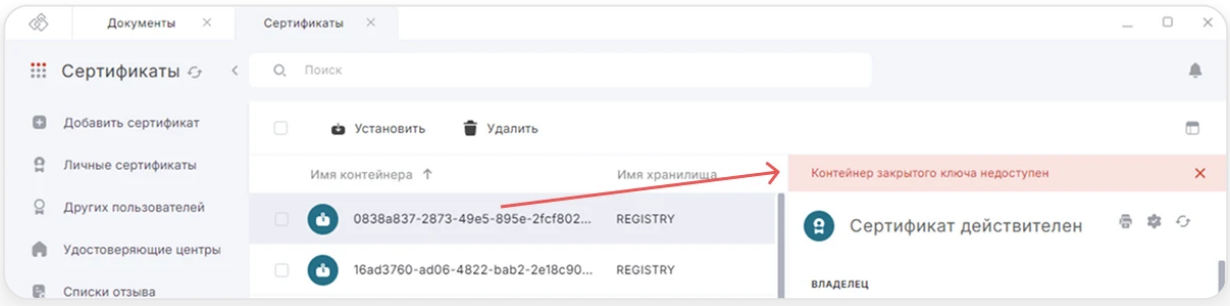
Проверка наличия закрытого ключа

> ⚠ **Примечание**: Данная функция доступна только для контейнеров, в которых есть сертификат.

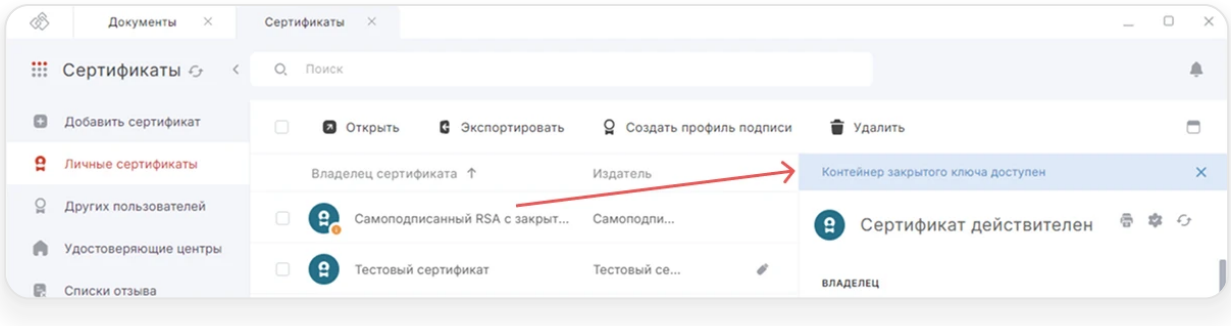
1. При необходимости подключите ключевой носитель к устройству.
2. Перейдите в раздел **Сертификаты** → **Ключи**.
3. Выделите контейнер в списке.
4. Нажмите на кнопку **Подробно** на панели действий.
5. Справа от списка откроется область со сведениями.
6. Нажмите на кнопку **Протестировать** .
7. При необходимости введите пароль к ключевому контейнеру.

Результаты проверки:

- Контейнер закрытого ключа недоступен.



- Контейнер закрытого ключа доступен.



Удаление контейнера

> ⚠️ **Примечание**: Удаленный контейнер не подлежит восстановлению! Вам придется перевыпускать сертификат.

1. Перейдите в раздел **Сертификаты** → **Ключи**.
2. Выделите контейнер в списке.
3. Нажмите кнопку **Удалить**.
4. Подтвердите удаление.

Если во время удаления был установлен флаг **Удалить связанный с контейнером сертификат**, то сертификат удалится из хранилища **Личные сертификаты**.

Обновление списка контейнеров

1. Перейдите в раздел **Сертификаты**.
2. Нажмите кнопку **Обновить** , размещенную рядом с заголовком раздела.

Возможные ошибки

При возникновении ошибки вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Описание	Рекомендуемые действия
Не удалось загрузить контейнеры	Отсутствует КриптоПро CSP	Установите криптопровайдер КриптоПро CSP и перезапустите приложение КриптоАРМ

Инструкции по теме

- Установка корневого и промежуточного сертификатов
- Экспорт личного сертификата
- Импорт сертификатов других пользователей

Открыть статью на сайте

Адресные книги

- Основные понятия
- Действия с адресными книгами

Основные понятия

Адресные книги в приложении предназначены для хранения и управления контактами, которые используются для отправки писем (в том числе зашифрованных) и для шифрования документов.

При установке приложения автоматически создаётся дефолтная локальная книга с названием «Контакты», в которую можно сразу добавлять записи.

Приложение поддерживает несколько типов адресных книг:

- **Локальная адресная книга** — хранит контакты на устройстве пользователя. Контакты можно добавлять вручную или загружать из файлов **vCard**.
- LDAP и ALD Pro — подключаемые корпоративные адресные книги.
- CardDAV — адресная книга, синхронизируемая с серверами по протоколу CardDAV.

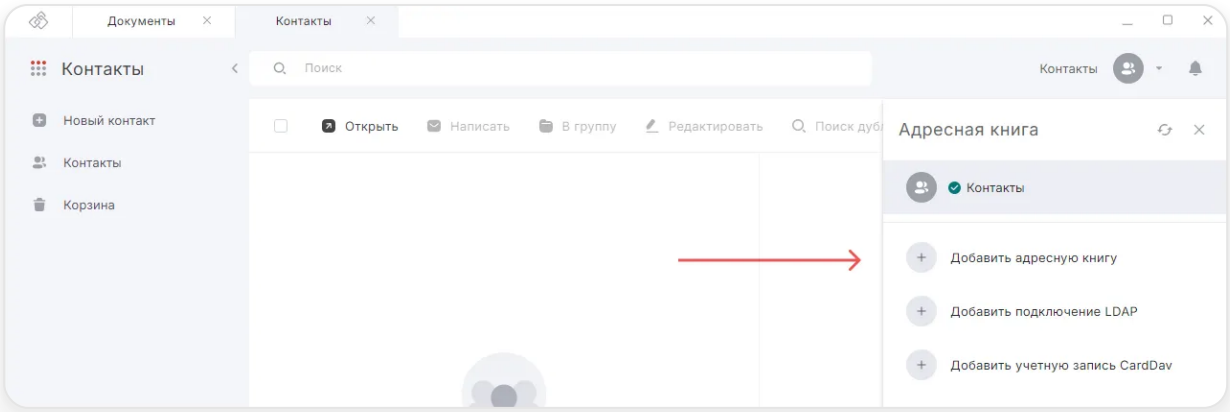
Контакты могут включать:

- ФИО, должность, телефоны и e-mail-адреса;
- Почтовые адреса и дату рождения;
- Фотографии, логотипы и мультимедийные элементы;
- Привязанные сертификаты.

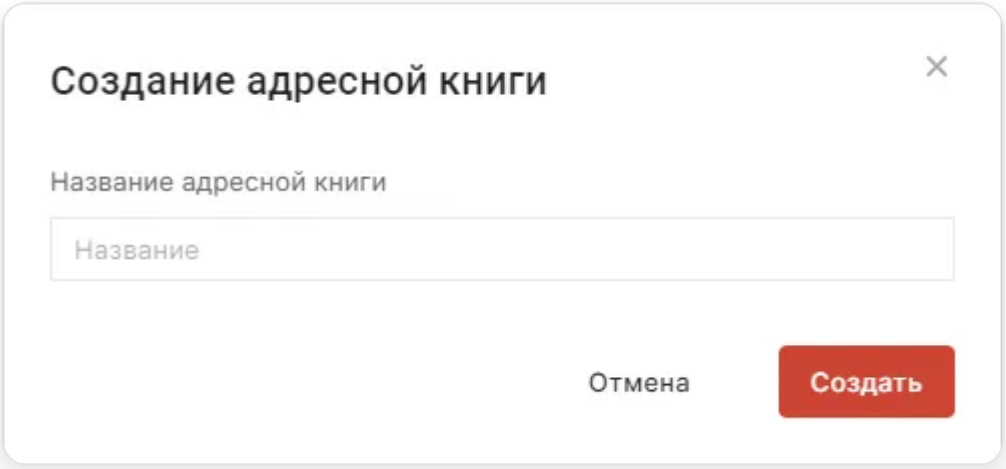
Действия с адресными книгами

Добавление книги

1. Откройте раздел **Контакты**.
2. Откройте окно со списком адресных книг. Для этого нажмите на название активной адресной книги в верхнем правом углу окна.
3. Нажмите **Добавить адресную книгу**.



4. Укажите название адресной книги.
5. Нажмите **Создать**.



💡 После создания новой адресной книги переключитесь на неё и добавьте контакты вручную или импортируйте их из файла.

Переключение между книгами

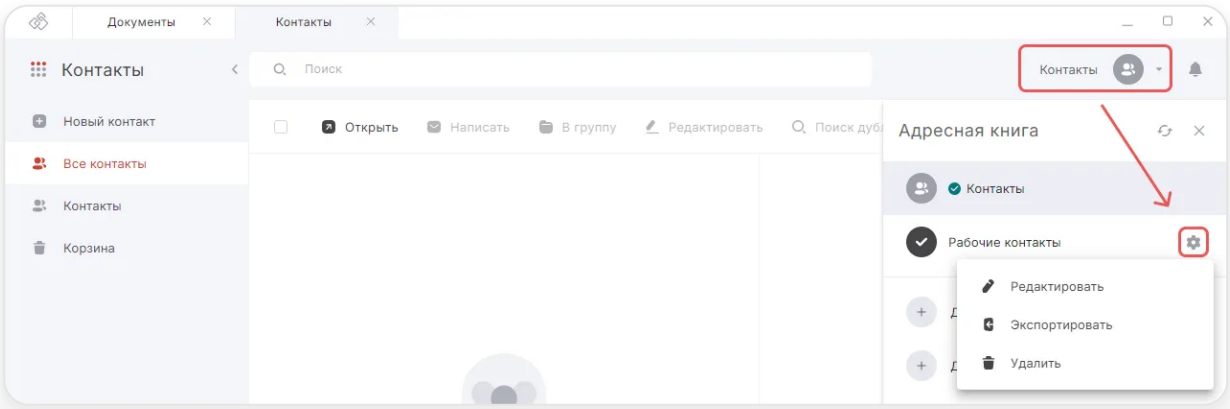
1. Откройте раздел **Контакты**.
2. Откройте окно со списком адресных книг. Для этого нажмите на название активной адресной книги в верхнем правом углу окна.
3. Выберите нужную адресную книгу из списка доступных.

Активная книга отмечается иконкой , список контактов автоматически обновляется в соответствии с выбранной книгой.

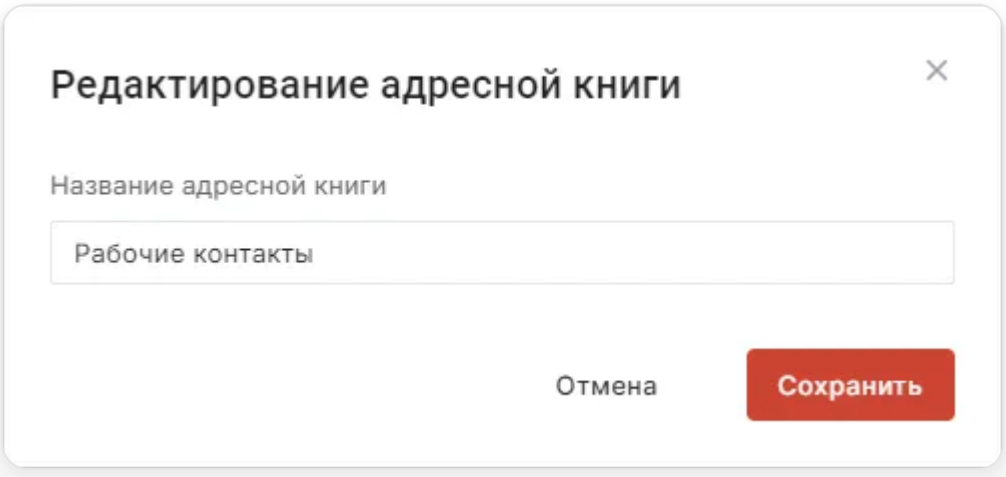
Редактирование книги

> ⚠️ **Примечание:** Редактировать можно только название адресной книги. Содержимое контактов редактируется отдельно.

1. Откройте раздел **Контакты**.
2. Откройте окно со списком адресных книг. Для этого нажмите на название активной адресной книги в верхнем правом углу окна.
3. Наведите курсор на панель с адресной книгой.
4. Нажмите на кнопку **Настройки** .



5. В появившемся меню выберите действие **Редактировать**.



6. Укажите новое название адресной книги.
7. Нажмите **Сохранить**.

Экспорт книги

> 💡 **Совет:** Можно экспортировать как всю адресную книгу, так и выбранные контакты.

1. Откройте раздел **Контакты**.
2. Откройте окно со списком адресных книг. Для этого нажмите на название активной адресной книги в верхнем правом углу окна.
3. Наведите курсор на панель с адресной книгой.
4. Нажмите на кнопку **Настройки** .
5. В появившемся меню выберите действие **Экспортировать**.
6. Укажите место и имя файла для сохранения.

Экспортируемый файл будет в формате **.vcf (vCard)**, включая все данные контакта и привязанные сертификаты (если они есть).

Удаление книги

> ⚠️ **Примечание:** Удаление книги приведёт к удалению всех контактов в локальной книге.

1. Откройте раздел **Контакты**.
2. Откройте окно со списком адресных книг. Для этого нажмите на название активной адресной книги в верхнем правом углу окна.
3. Наведите курсор на панель с адресной книгой.
4. Нажмите на кнопку **Настройки** .
5. В появившемся меню выберите действие **Удалить**.
6. Подтвердите удаление в появившемся окне.

Инструкции по теме

- Действия с локальными контактами
- Привязка сертификата к контакту
- Добавление адресной книги LDAP
- Добавление адресной книги ALD Pro

Открыть статью на сайте

Добавление контакта

- Создание контакта
- Описание полей контакта

Общая информация

В КриптоАРМ можно создать контакт с расширенным профилем, который будет включать:

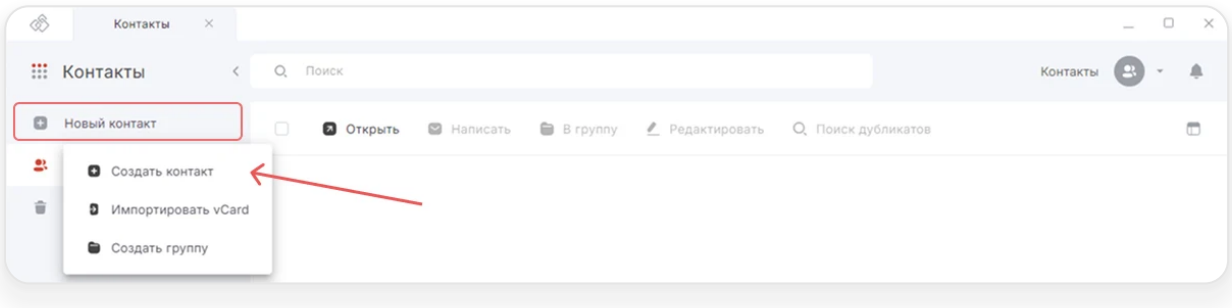
- Личные данные (ФИО, должность, компания)
- Различные контактные данные (телефоны, email, адреса)
- Фотографии, загруженные вручную или полученные из сервиса Gravatar
- Сертификаты для безопасной переписки

> 💡 **Совет**: Сертификаты в профиле контакта можно использовать для шифрования сообщений и файлов при отправке.
>
> 🔍 Gravatar (от англ. globally recognized avatar — глобально распознаваемый аватар) — сервис компании Automattic, позволяющий интернет-пользователям хранить свой аватар на специальном сервере.

Создание контакта

Способ 1: Создание из раздела "Контакты"

1. Перейдите в раздел **Контакты**.
2. Переключитесь на необходимую адресную книгу.
3. Нажмите на кнопку **Новый контакт** в боковом меню.
4. В появившемся меню выберите **Создать контакт**.

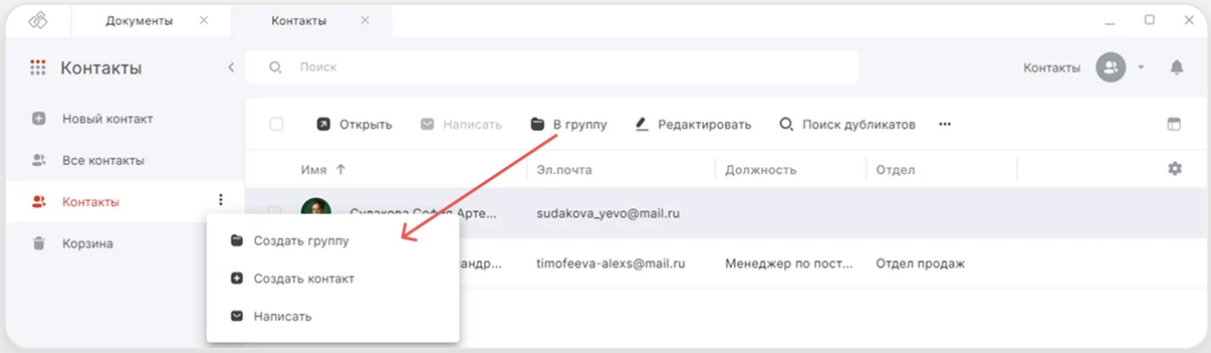


5. Откроется форма создания контакта.

6. Заполните данные о контакте.
7. Добавьте фото контакта. Подробнее в инструкции Настройка аватаров.
8. При необходимости добавьте электронный сертификат. Подробнее в инструкции Привязка сертификата к контакту.
9. Нажмите кнопку **Сохранить**.

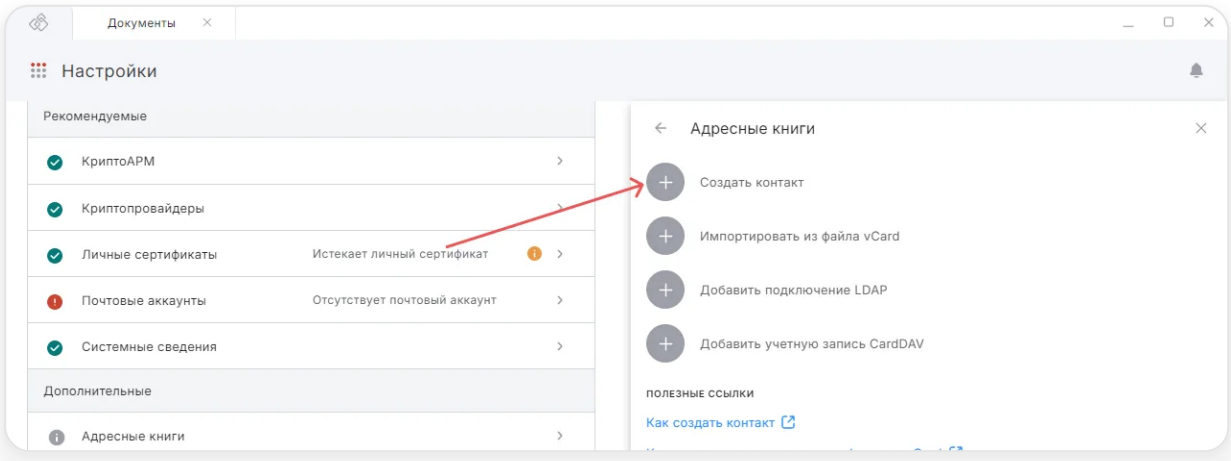
Контакт будет добавлен в корневую группу адресной книги.

> 💡 **Совет**: Чтобы создать контакт в определенной группе, нажмите на кнопку **Еще** ⋮ на панели с группой в боковом меню. Затем выберите **Создать контакт**.



Способ 2: Создание из раздела "Настройки"

1. Перейдите в раздел **Настройки** → проверка **Адресные книги**.
2. Откроется окно со списком адресных книг (если они обнаружены).
3. Нажмите на кнопку **Добавить** ⊕ в верхней части окна.
4. Выберите действие **Создать контакт**.

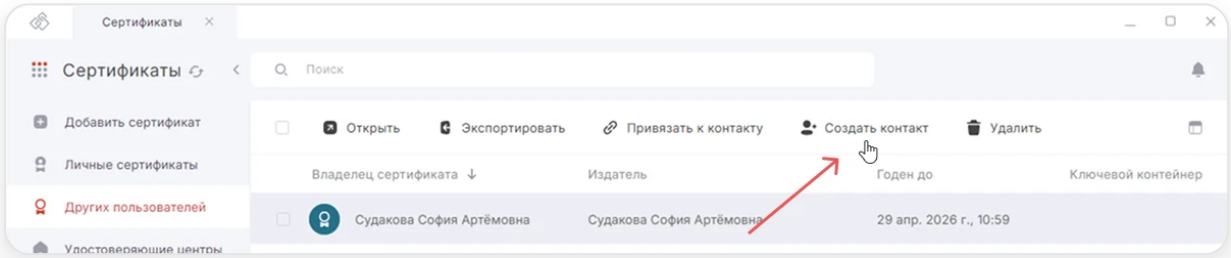


5. Откроется новая вкладка с формой создания контакта.

6. Следуйте шагам из инструкции Способ 1: Создание из раздела "Контакты".

Способ 3: Создание из сертификата

1. Перейдите в раздел **Сертификаты** → **Других пользователей**.
2. Выделите сертификат в списке.
3. Нажмите **Создать контакт** на панели действий.



4. Откроется форма создания контакта. Данные будут автоматически заполнены на основе сертификата. Сертификат будет привязан к контакту.
5. При необходимости внесите изменения в в данные.
6. Добавьте фото контакта. Подробнее в инструкции Настройка аватаров.
7. Нажмите **Сохранить**.

Контакт будет добавлен в корневую группу адресной книги.

Описание полей контакта

Раздел	Поле	Тип данных	Обязательное	Описание
Личная информация	Фото	Изображение (JPG/ webp)	Нет	Аватар контакта (макс. 2MB)
	Фамилия	Текст	Нет	
	Имя	Текст	Да	
	Отчество	Текст	Нет	
Рабочие данные	Организация	Текст	Нет	Название компании
	Подразделение	Текст	Нет	Отдел/ Департамент
	Должность	Текст	Нет	
	Номер телефона	Телефон	Нет	

Раздел	Поле	Тип данных	Обязательное	Описание
Контактные данные				Формат: +7 (XXX) XXX-XX-XX
	Адрес электронной почты	Email	Нет	-
Дополнительно	Дата рождения	Дата	Нет	Формат: ДД.ММ.ГГГГ
	Адрес	Текст	Нет	Регион, город, улица, дом, индекс
	Примечание	Текст	Нет	Произвольные заметки
Сертификат	Привязанные сертификаты	Сертификаты	Нет	Сертификат из файла .cer, .crt или из раздела **Сертификаты → Других пользователей**

Инструкции по теме

- Привязка сертификата к контакту
- Действия с локальными контактами
- Добавление адресной книги LDAP
- Добавление адресной книги ALD Pro

Открыть статью на сайте

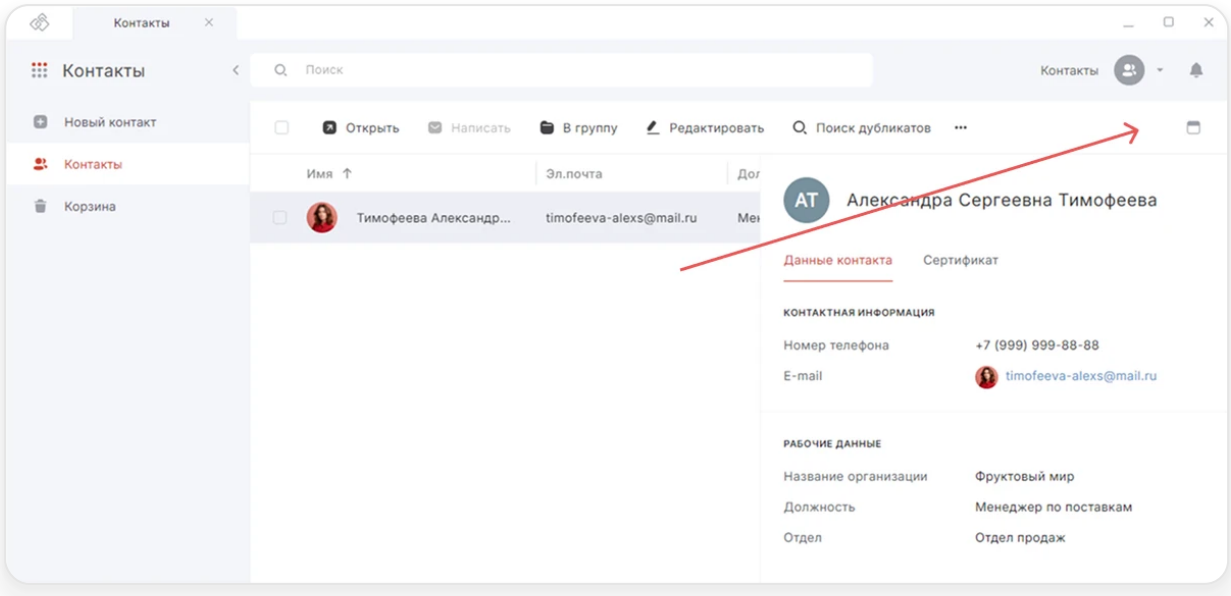
Действия с контактами

- Просмотр информации о контакте
- Редактирование контакта
- Поиск контакта
- Экспорт контакта
- Отправка по почте
- Удаление контакта
- Восстановление удаленных контактов

Просмотр информации о контакте

Быстрый просмотр

1. Перейдите в раздел **Контакты**.
2. Переключитесь на необходимую адресную книгу.
3. Нажмите на панель с контактом в списке контактов.
4. Нажмите кнопку **Просмотр** на панели действий.

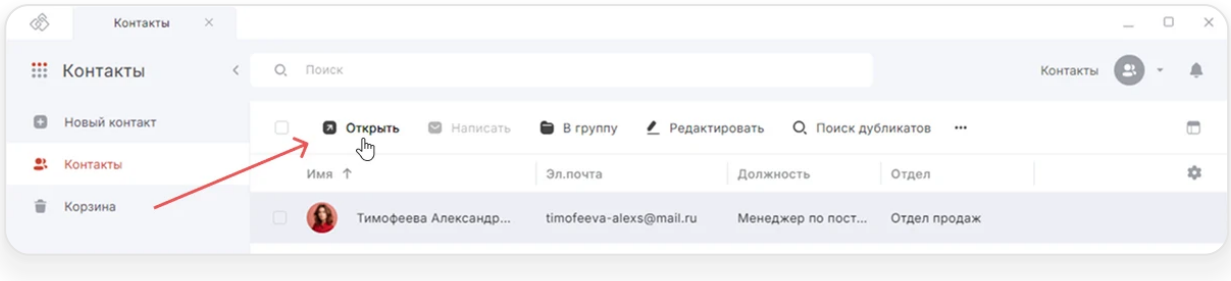


5. Справа от списка контактов откроется область со сведениями о контакте.

Просмотр в новой вкладке

1. Перейдите в раздел **Контакты**.
2. Выделите контакт в списке.

3. Нажмите кнопку **Открыть** на панели действий.

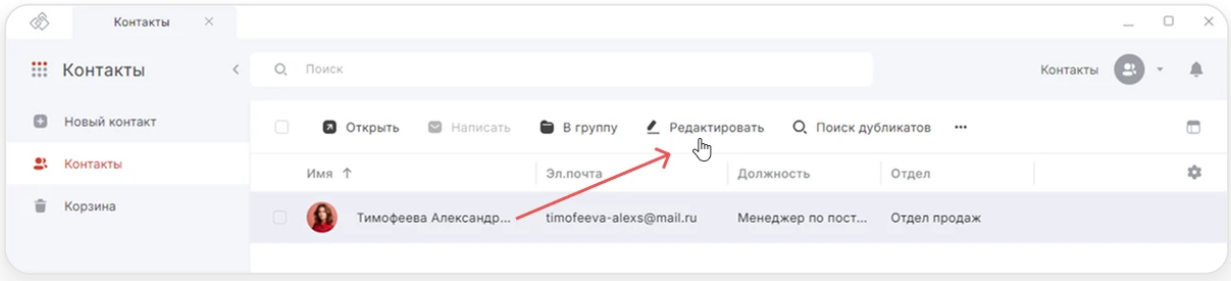


Информация о контакте откроется в новой вкладке.

Редактирование контакта

> ⚠ **Примечание**: Для редактирования доступны только локальные контакты.

1. Перейдите в раздел **Контакты**.
2. Переключитесь на необходимую адресную книгу.
3. Выделите в списке контакт, данные которого необходимо отредактировать.
4. Нажмите кнопку **Редактировать** в верхней панели.



5. Внесите изменения в данные контакта.
6. Нажмите **Сохранить**.

Поиск контакта

> ⚠ **Примечание**: Поиск контактов осуществляется в активной адресной книге.

Чтобы найти определенный контакт:

1. Перейдите в раздел **Контакты**.
2. Откройте необходимую адресную книгу.
3. В поисковой строке введите параметры поиска.

Поиск возможен по следующим значениям: ФИО, e-mail, номер телефона.

Экспорт контакта

> 💡 **Совет**: Можно экспортировать как всю адресную книгу целиком, так и только выбранные контакты — это удобно при передаче данных коллегам или миграции на другую систему.

1. Перейдите в раздел **Контакты**.
2. Переключитесь на необходимую адресную книгу.
3. Выделите в списке один или несколько контактов.
4. Нажмите кнопку **Экспортировать** в верхней панели.
5. В файловом менеджере укажите место сохранения файла.

Контакты сохраняются в формате `.vcf` (vCard).

> 📌 Экспорт контактов доступен также для контактов, получаемых из LDAP-адресной книги.

Что сохраняется при экспорте

В экспортируемом файле vCard могут быть записаны:

- ФИО и должность
- номера телефонов и e-mail-адреса
- название организации и подразделения
- почтовые адреса
- день рождения и дополнительные заметки
- фотографии (если добавлены в профиль)
- сертификаты контакта

> 🔐 Если у контакта несколько сертификатов, то сохраняются все.

Отправка по почте

> ⚠️ Примечание: Для отправки профилей подписи по почте в приложении должен быть подключен почтовый аккаунт.

1. Перейдите в раздел **Контакты**.
2. Переключитесь на необходимую адресную книгу.
3. Выделите в списке один или несколько контактов.
4. Нажмите кнопку **Отправить контакт** в верхней панели.
5. Откроется вкладка с письмом, в которой выбранные контакты будут автоматически добавлены во вложение в формате `.vcf` (vCard).
6. Укажите получателя, при необходимости добавьте текст письма и нажмите **Отправить**.

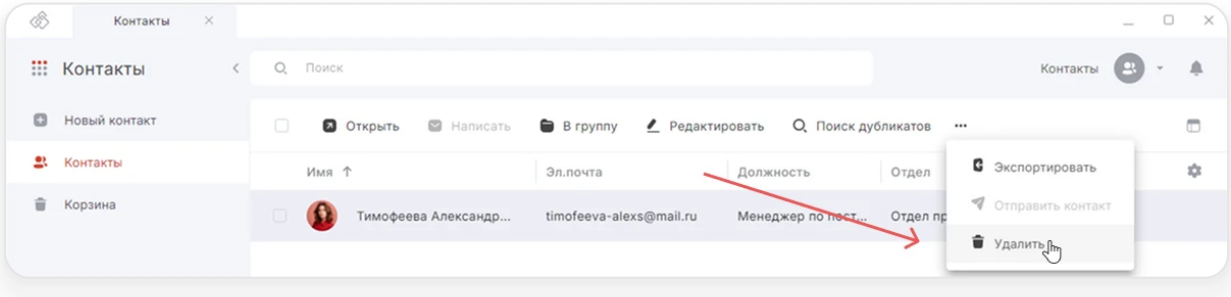
Удаление контакта

Удаленные контакты хранятся в группе «Корзина».

> ⚠️ **Примечание**: Удалить можно только локальные контакты. Контакты из внешних адресных книг будут удалены при удалении самой книги.

Стандартный способ

1. Перейдите в раздел **Контакты**.
2. Выделите контакт в списке.
3. Нажмите кнопку **Удалить** на панели действий.



Выбранный контакт будет перемещен в **Корзину**.

Групповое удаление

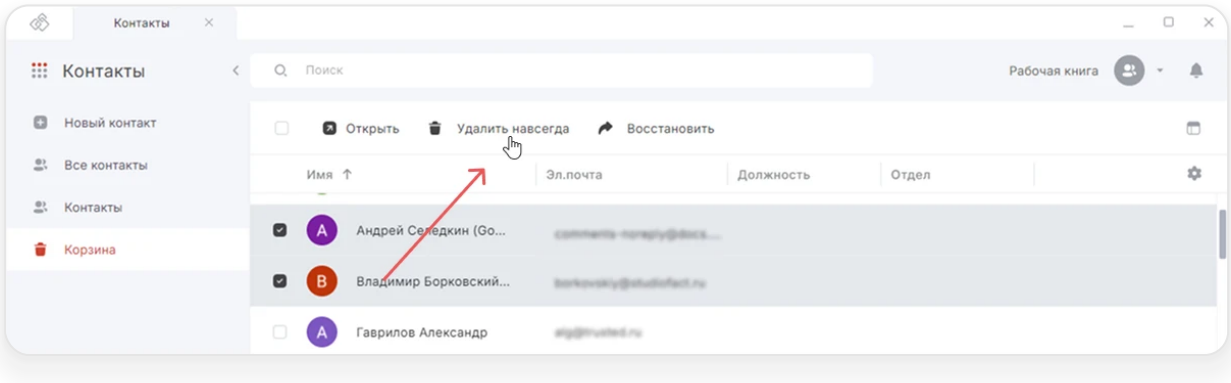
1. Перейдите в раздел **Контакты**.
2. Отметьте флажками контакты, которые необходимо удалить.

3. Нажмите кнопку **Удалить** на панели действий.

Выбранные контакты будут перемещены в **Корзину**.

Удаление из «Корзины»

1. Перейдите в раздел **Контакты** → **Корзина**.
2. Отметьте флажками контакты, которые необходимо навсегда удалить.
3. Нажмите **Удалить навсегда** на панели действий.



Выбранные контакты будут удалены из приложения.

> 💡 **Совет**: Чтобы очистить «Корзину», установите флажки для всех контактов в списке и нажмите на кнопку **Удалить навсегда** на панели действий.

Восстановление удаленных контактов

После переноса контакта в «Корзину» его можно восстановить.

1. Перейдите в раздел **Контакты** → **Корзина**.
2. Отметьте флажками контакты, которые необходимо восстановить.
3. Нажмите на кнопку **Восстановить** на панели действий.

Контакт будет восстановлен в группу, из которой был удален.

Инструкции по теме

- Создание локального контакта
- Действия с локальными контактами
- Настройка аватаров

Открыть статью на сайте

Настройка аватаров

- Возможности
- Способы добавления фото
- Удаление фото

Возможности

Вы можете персонализировать контакты, добавив к ним изображения одним из способов:

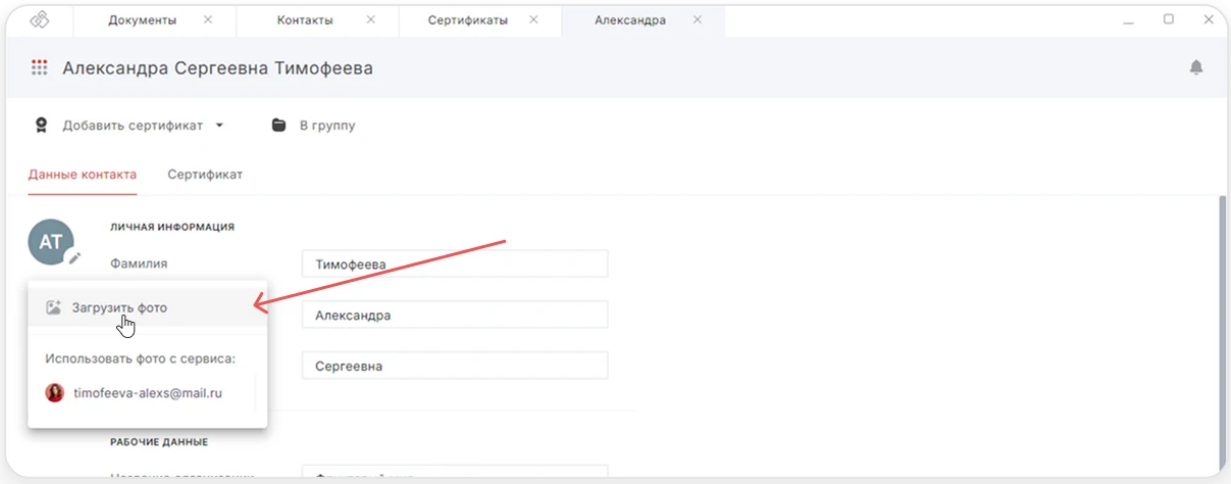
- **Загрузка с компьютера** - используйте собственные фотографии,
- **Сервис Gravatar** - автоматическое получение аватара с сервиса Gravatar.

> 🔍 Gravatar (от англ. globally recognized avatar — глобально распознаваемый аватар) — сервис компании Automattic, позволяющий интернет-пользователям хранить свой аватар на специальном сервере.
>
> 🚨 При экспорте контакта с фотографией в формате `.vcf`, изображение переносится вместе с данными. То же самое происходит и при импорте: если контакт содержит фото в `.vcf`, оно будет загружено вместе с остальными сведениями. Подробнее про поддержку vCard читайте в инструкции.

Способы добавления фото

1. Загрузка фото с компьютера

1. Перейдите в раздел **Контакты**.
2. Откройте форму создания или редактирования контакта.
3. Нажмите на аватар контакта.
4. В открывшемся меню выберите действие **Загрузить фото**.



5. Откроется окно файлового менеджера.
6. Укажите путь к файлу с фото.

> ⚠️ **Примечание**: Для выбора доступны файлы в формате `jpg (jpeg)`, `gif`, `webp`, `bmp` и размером не более 2МБ.

7. Нажмите **Сохранить** в форме редактирования контакта.

Фотография станет аватаркой контакта и будет отображаться во всех разделах приложения.

2. Установка фото из сервиса Gravatar

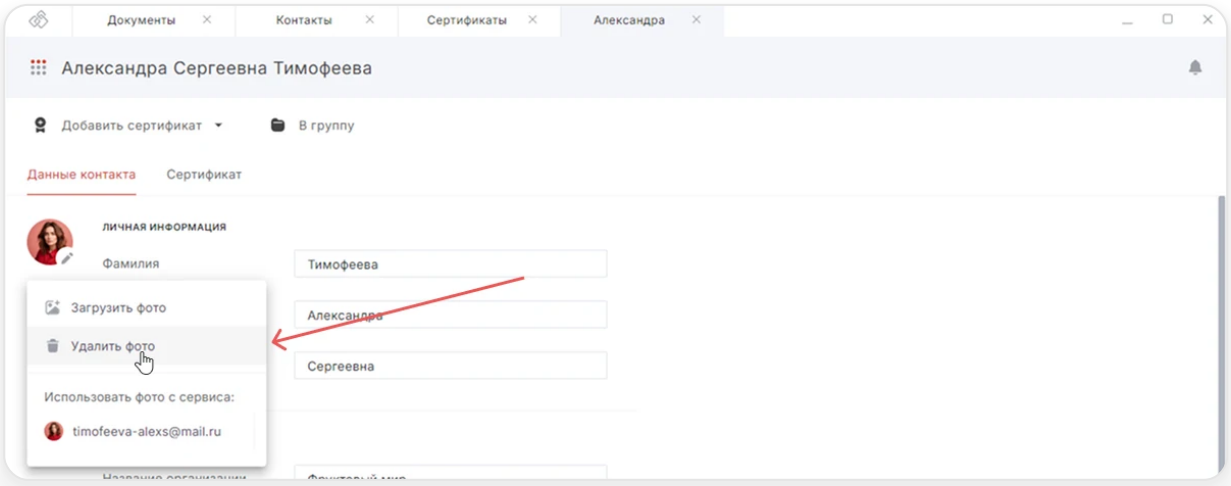
> ⚠️ **Примечание**: Адрес электронной почты, сохраненный в контакте, должен совпадать с адресом пользователя, зарегистрированным на сервисе Gravatar. Если адреса не совпадают, то аватар отображаться не будет.

1. Перейдите в раздел **Контакты**.
2. Откройте форму создания или редактирования контакта.
3. Нажмите на аватар контакта.
4. Откроется меню действий с аватаром контакта. В меню будут отображены фото, полученные с сервиса Gravatar.
5. Выберите фото.
6. Нажмите **Сохранить** в форме редактирования контакта.

Фотография станет аватаркой контакта и будет отображаться во всех разделах приложения.

Удаление фото

1. Перейдите в раздел **Контакты**.
2. Откройте форму редактирования контакта.
3. Нажмите на аватар контакта.
4. Откроется меню действий с аватаром контакта.
5. Выберите действий **Удалить фото**.



Инструкции по теме

- Как создать локальный контакт
- Действия с локальными контактами
- Как добавить адресную книгу LDAP
- Как добавить адресную книгу ALD Pro

Открыть статью на сайте

Настройка сертификатов

- Привязка сертификатов к контакту
- Управление сертификатами контакта

Привязка сертификатов к контакту

Для безопасного обмена зашифрованными письмами и документами в приложении необходимо привязать сертификат к контакту.

Общие особенности

1. Привязка сертификатов доступна только для **локальных** контактов. Контакты из внешних источников (LDAP, ALD Pro и др.) редактируются на стороне сервера.
2. Сертификаты имеют срок действия. При перевыпуске обязательно замените их у контактов, чтобы обмен сообщениями продолжался без ошибок.
3. При наличии у контакта нескольких сертификатов приложение автоматически использует тот, который поддерживает выбранный алгоритм шифрования.

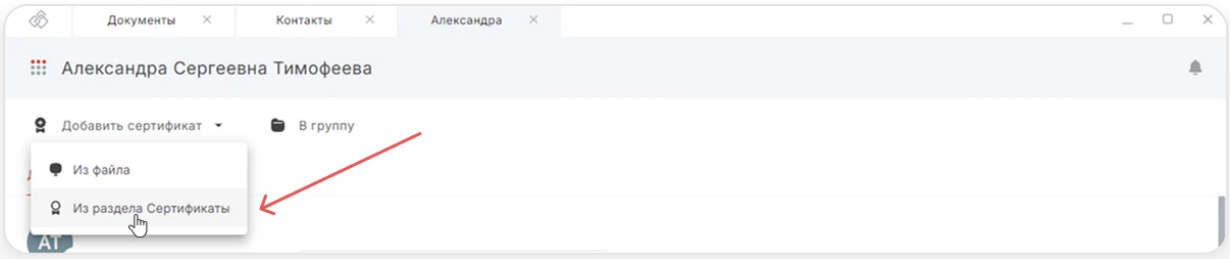
> ⚠️ **Примечание**: Удаление сертификатов контакта возможно только при редактировании. Это позволяет избежать случайного удаления важных данных при просмотре информации.

Способы привязки сертификата

1. Из хранилищ

К контакту можно привязать сертификаты из хранилищ **Личные сертификаты** и сертификаты **Других пользователей**.

1. Откройте создание или редактирование контакта.
2. Нажмите кнопку **Добавить сертификат**.
3. В открывшемся меню выберите действие **Из раздела Сертификаты**.



4. Откроется окно со списком сертификатов из хранилищ **Личные сертификаты** и **Других пользователей**.

5. Выберите сертификат, нажав на иконку сертификата. Возможен множественный выбор. После выбора сертификат автоматически добавится в список сертификатов контакта.
6. После выбора закройте окно со списком сертификатов.
7. Нажмите кнопку **Сохранить**.

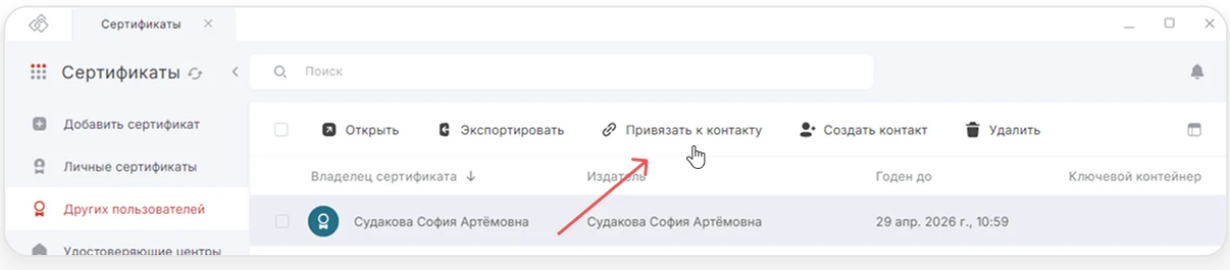
2. Из файла

1. Откройте создание или редактирование контакта.
2. Нажмите кнопку **Добавить сертификат**.
3. В открывшемся меню выберите действие **Из файла**.
4. Откроется окно файлового менеджера.
5. Выберите файл с сертификатом .cer или .crt.
6. После выбора сертификат автоматически добавится в список сертификатов контакта.
7. Нажмите кнопку **Сохранить**.

3. В разделе «Сертификаты»

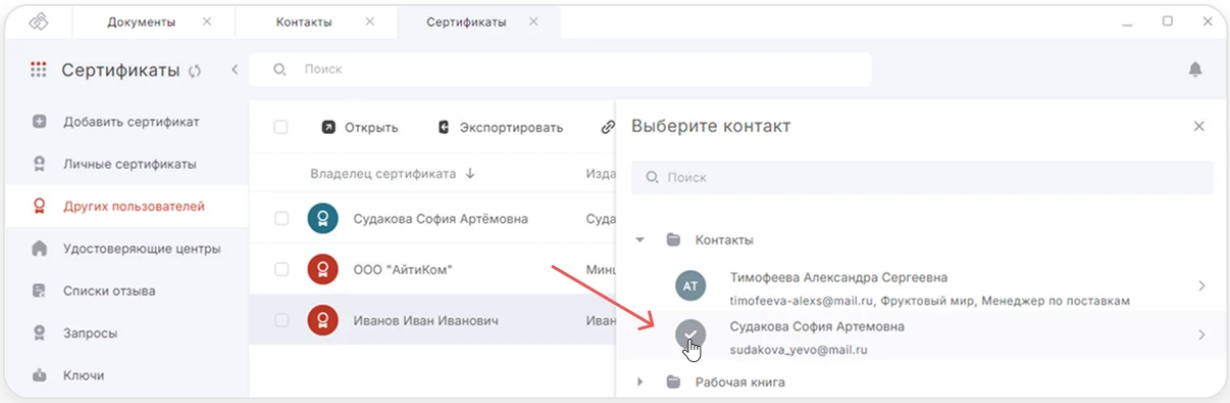
1. Перейдите в раздел **Сертификаты** → **Других пользователей**.
2. Выделите сертификат в списке.

3. Нажмите на кнопку **Привязать к контакту** на панели действий.



4. Откроется окно **Выберите контакт**.

5. Выберите контакт, нажав на его аватар.



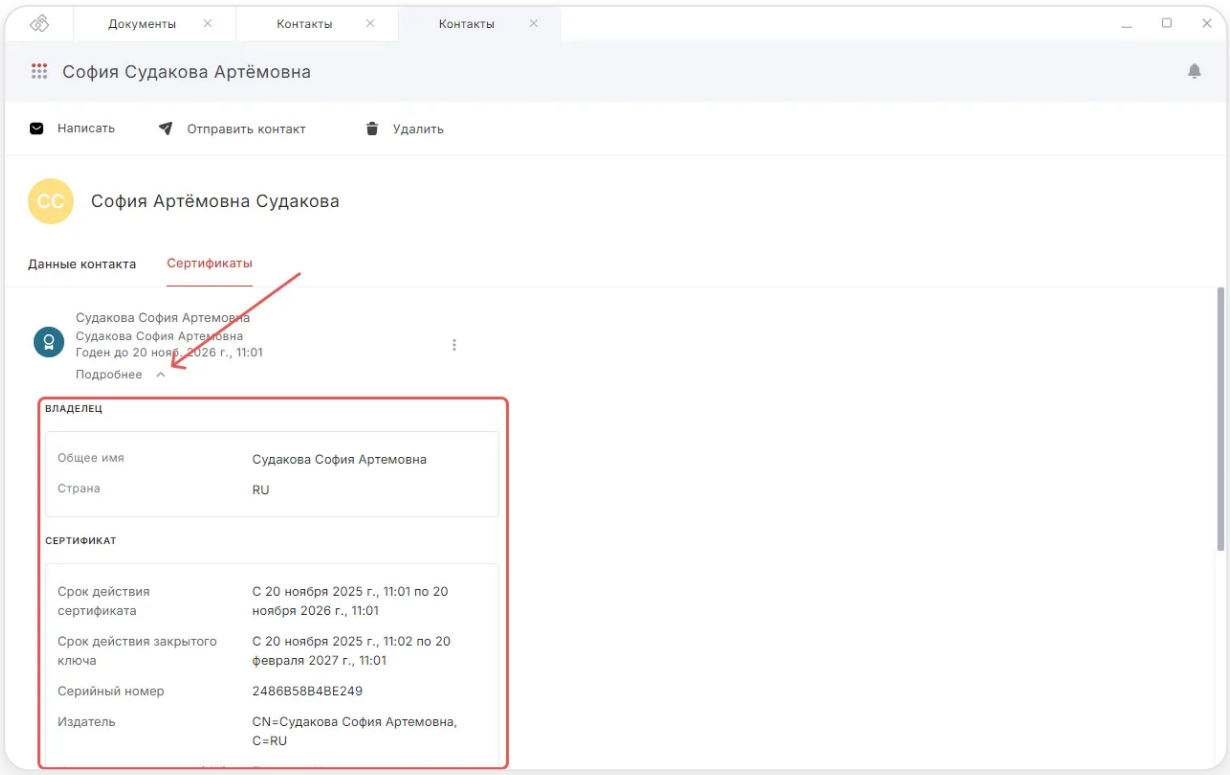
6. Подтвердите действие в модальном окне.

Сертификат успешно привязан к контакту.

Управление сертификатами контакта

Просмотр сведений о сертификате

1. Откройте профиль контакта с привязанным сертификатом любым из способов.
2. Перейдите на вкладку **Сертификаты**.
3. Нажмите на кнопку **Подробнее** на панели с сертификатом.



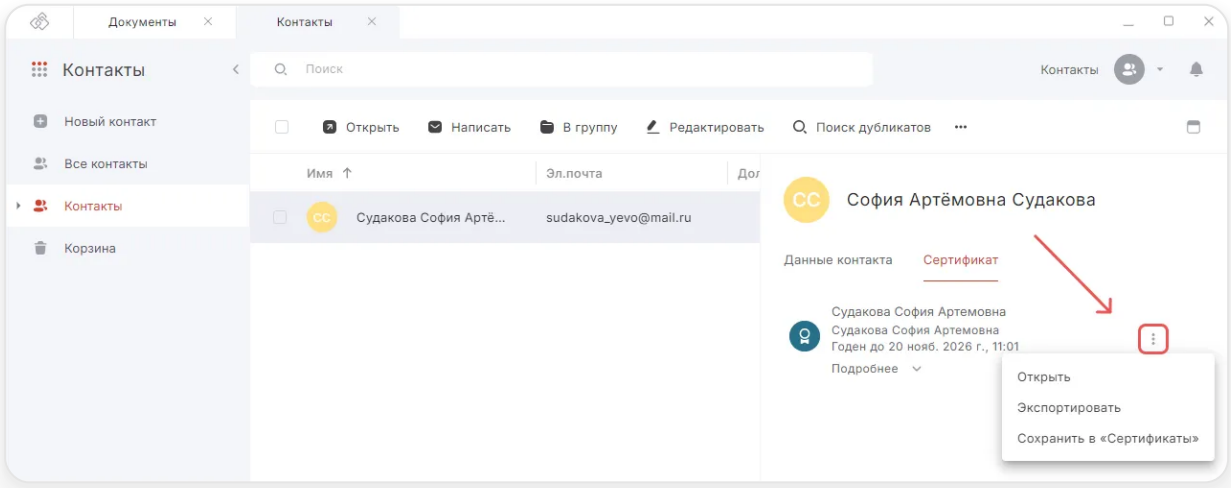
Отобразятся полные технические сведения, включая срок действия и назначение.

> 📌 Для просмотра встроенными средствами Windows нажмите **Еще** → **Открыть**.

Экспорт сертификата в файл

> 💡 Удобно, если сертификат нужно передать или загрузить в другое приложение.

1. Откройте профиль контакта с привязанным сертификатом любым из способов.
2. Перейдите на вкладку **Сертификаты**.
3. Нажмите на кнопку **Еще** на панели с сертификатом.
4. Выберите действие **Экспортировать**.



5. В файловом менеджере укажите место сохранения файла.

Сертификат будет выгружен в формате .cer.

Сохранение в хранилище «Других пользователей»

> 💡 Используйте, если сертификат контакта ещё не сохранён в системе.

1. Откройте профиль контакта с привязанным сертификатом любым из способов.
2. Перейдите на вкладку **Сертификаты**.
3. Нажмите на кнопку **Еще** на панели с сертификатом.
4. Выберите действие **Сохранить в «Сертификаты»**.

Сертификат контакта будет сохранен в хранилище **Сертификаты других пользователей** раздела **Сертификаты**.

Инструкции по теме

- Создание локального контакта
- Действия с локальными контактами
- Настройка аватаров

Открыть статью на сайте

Группировка контактов

- Создание новых групп
- Действия с группой

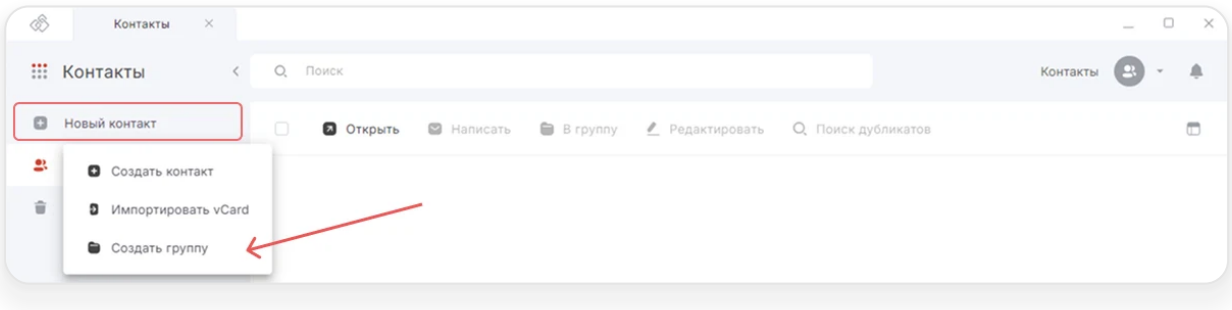
Создание новых групп

Группировка контактов помогает удобно организовать вашу адресную книгу. Можно разделить контакты по разным критериям: профессии (коллеги, клиенты, партнёры), проектам или отделам.

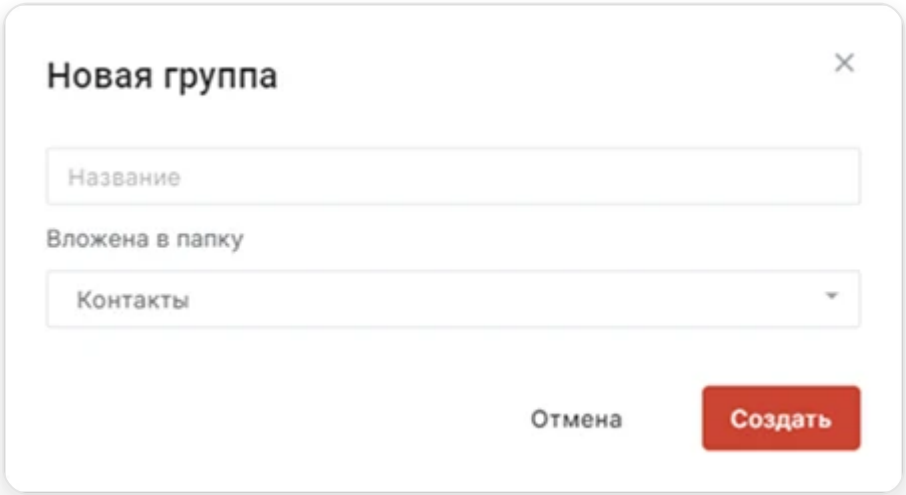
Система поддерживает многоуровневую вложенность групп для детальной классификации.

1. Стандартный способ

1. Перейдите в раздел **Контакты**.
2. Переключитесь на необходимую адресную книгу.
3. Нажмите на кнопку **Новый контакт** в боковом меню.
4. Выберите **Создать группу**.



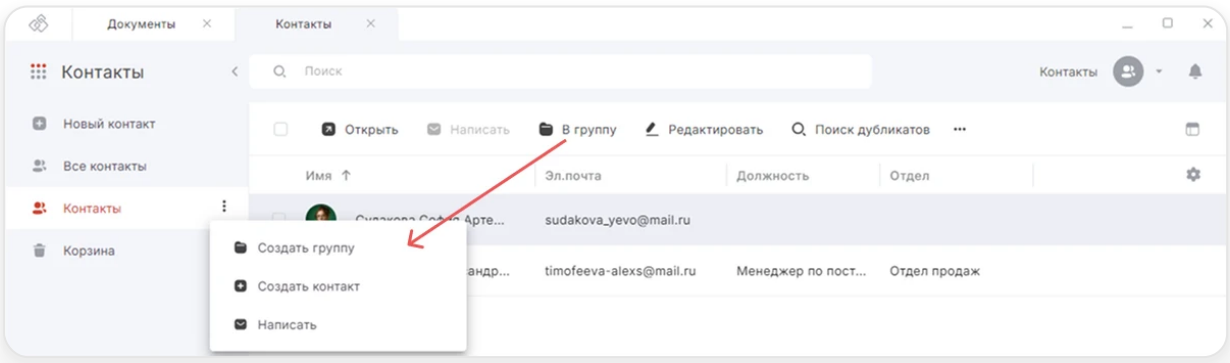
5. В открывшемся окне укажите название группы и уровень вложенности (в **Контакты** или в ранее созданную группу).



6. Нажмите **Создать**.

2. Создание вложенных групп

1. Перейдите в раздел **Контакты**.
2. Переключитесь на необходимую адресную книгу.
3. Вызовите контекстное меню по кнопке **Еще** , размещенной на панели с родительской группой в боковом меню.



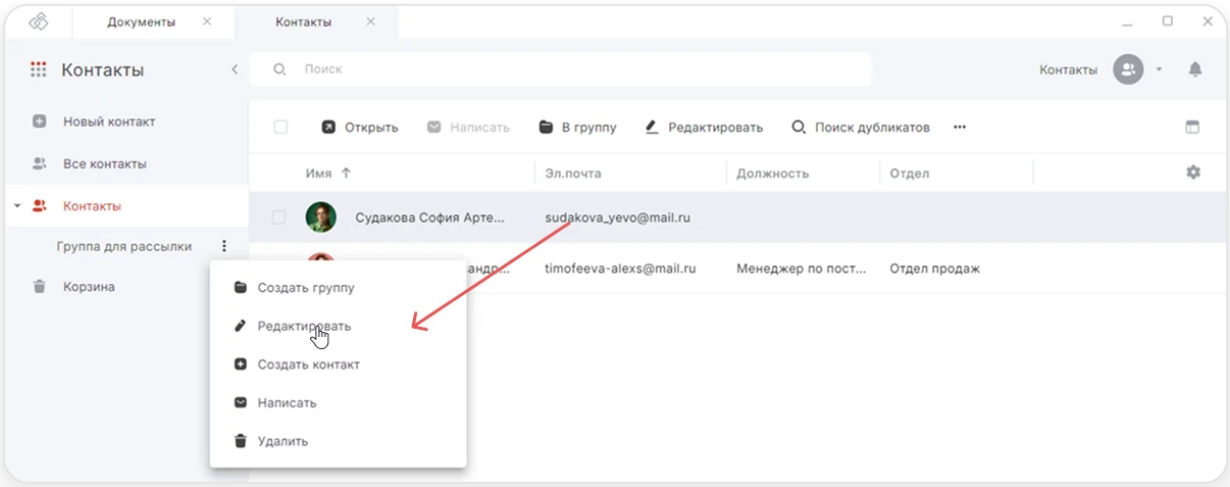
4. В открывшемся окне укажите название группы.
5. При необходимости настройте уровень вложенности.
6. Нажмите **Создать**.

Действия с группой

1. Редактирование группы

1. Перейдите в раздел **Контакты**.
2. Переключитесь на необходимую адресную книгу.

3. Вызовите контекстное меню по кнопке **Еще** , размещенной на панели с группой в боковом меню.
4. Выберите действие **Редактировать**.
5. Внесите изменения и нажмите **Сохранить**.



2. Отправка писем всей группе

1. Перейдите в раздел **Контакты**.
2. Переключитесь на необходимую адресную книгу.
3. Вызовите контекстное меню по кнопке **Еще** , размещенной на панели с группой в боковом меню.
4. Выберите действие **Написать**.
5. Откроется вкладка с **Новым сообщением**, в котором в поле получатели будут указаны все контакты, состоящие в группе.
6. Укажите содержимое письма и нажмите на **Отправить**.

3. Удаление группы

> ⚠️ **Примечание**: При удалении группы будут удалены все ее подгруппы и контакты.

1. Перейдите в раздел **Контакты**.
2. Переключитесь на необходимую адресную книгу.
3. Вызовите контекстное меню по кнопке **Еще** , размещенной на панели с группой в боковом меню.
4. Выберите действие **Удалить**.
5. Подтвердите удаление группы.

Группа будет удалена, а все ее контакты перемещены в **Корзину**.

Инструкции по теме

- Создание локального контакта
- Действия с локальными контактами
- Настройка аватаров

Открыть статью на сайте

Адресная книга LDAP

- Основные понятия
- Добавление книги LDAP
- Редактирование книги LDAP
- Удаление книги LDAP
- Возможные ошибки

Основные понятия

КриптоАРМ поддерживает интеграцию с корпоративными LDAP-каталогами, что позволяет импортировать контакты из Active Directory и автоматически синхронизировать изменения.

Принцип работы

1. КриптоАРМ подключается к серверу LDAP с использованием учетной записи пользователя, предназначенной для чтения каталога.
2. По заданной базе поиска и фильтру извлекаются контакты.
3. Полученные записи отображаются в интерфейсе КриптоАРМ как отдельная адресная книга.
4. При включенном автообновлении изменения на сервере автоматически отражаются в КриптоАРМ.

> 💡 Адресная книга LDAP не заменяет локальные контакты, а дополняет их. Можно использовать несколько адресных книг одновременно и комбинировать их с локальными контактами.

Добавление книги LDAP

Шаг 1. Настройка LDAP

1. Создайте в LDAP учетную запись, с которой будет выполняться подключение к серверу.
2. Настройте фильтры. В зависимости от настроек клиента, могут использоваться фильтры, в которых можно отсечь ненужные записи.
3. Сервер LDAP должен быть доступен по сети с компьютера, на котором работает почтовый клиент.

Если данный сервер находится за NAT или он закрыт брандмауэром, то необходимо обеспечить доступ по следующим портам:

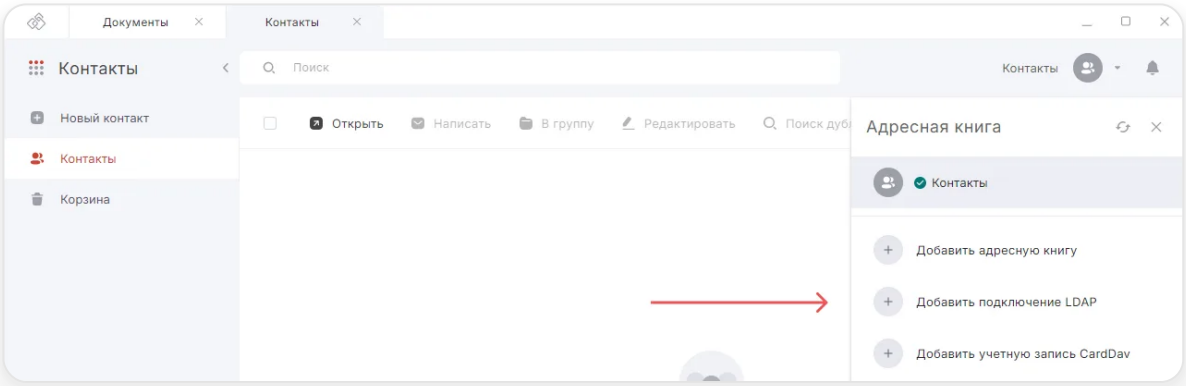
- 389 tcp или udp. Незащищенный доступ к активному каталогу.
- 636 tcp или udp. Доступ с защитой SSL.

Достаточно открыть и использовать один из данных портов, желательно 636.

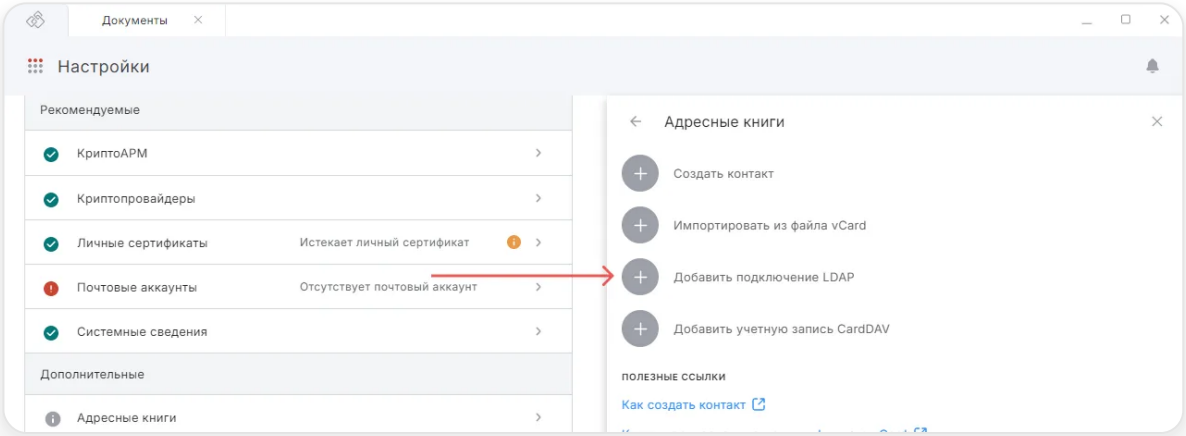
Шаг 2. Создание подключения в КриптоАРМ

1. Откройте форму подключения:

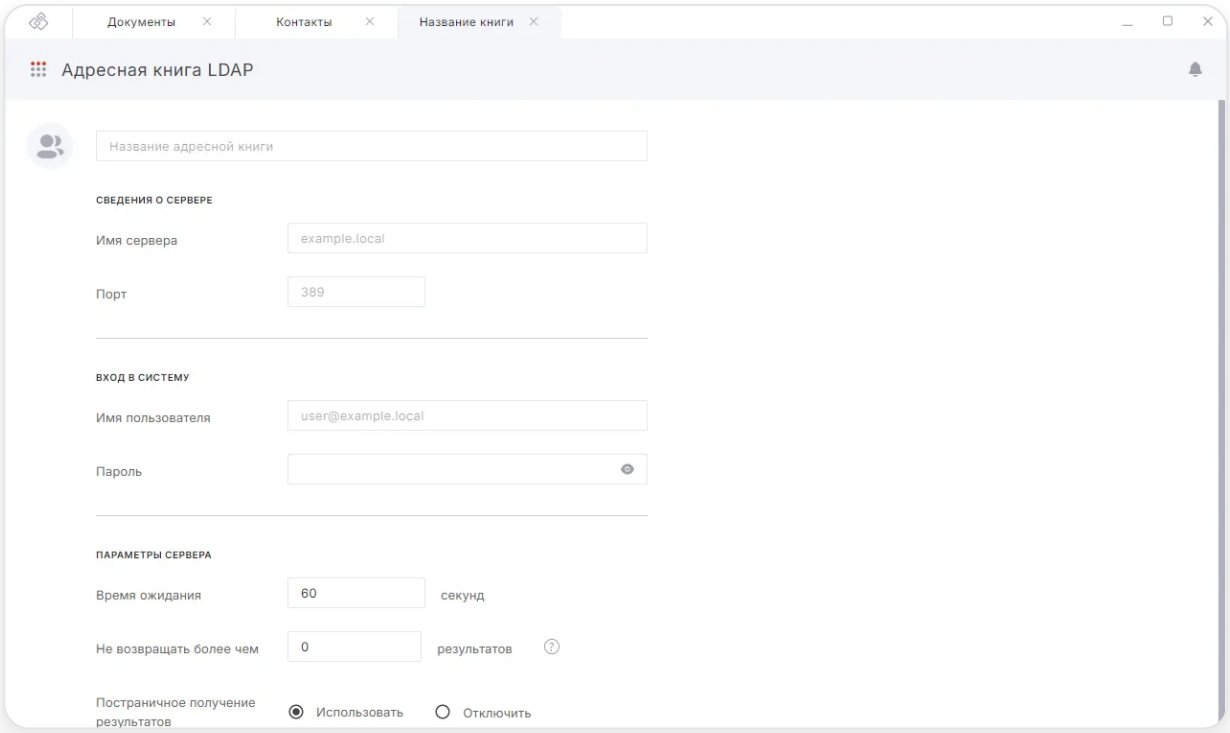
   - Перейдите в раздел **Контакты**. Откройте окно со списком адресных книг. Для этого нажмите на название активной адресной книги в верхнем правом углу окна. Выберите действие **Добавить подключение LDAP**.



   - Перейдите в раздел **Настройки** → проверка **Адресные книги**. Нажмите на кнопку **Добавить** в верхней части окна и выберите действие **Добавить подключение LDAP**.



2. Откроется форма подключения адресной книги.



3. Укажите параметры подключения.

4. Нажмите **Сохранить**.

> 💡 После подключения появится новая адресная книга. Чтобы увидеть её контакты, переключитесь на неё.

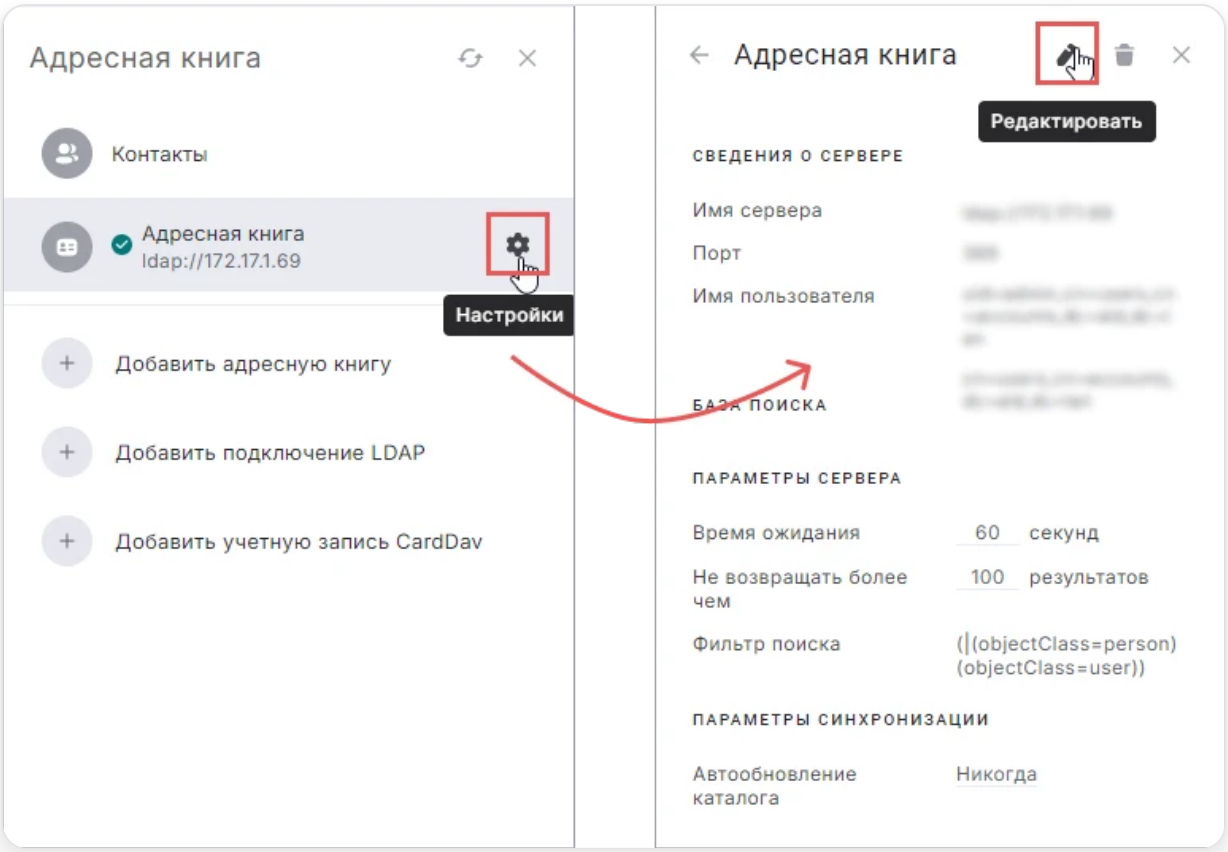
Описание параметров подключения

Название поля	Описание	Варианты выбора	По умолчанию
Название адресной книги	Имя книги, отображаемое в приложении.	Любое текстовое	—
Имя сервера	Адрес LDAP-сервера для подключения.	IP-адрес или доменное имя	—
Порт	Порт для подключения к LDAP-серверу.	—	—
Имя пользователя	Учетная запись для подключения к серверу.	—	—
Пароль	Пароль для указанной учетной записи.	—	—

Название поля	Описание	Варианты выбора	По умолчанию
Время ожидания	Время ожидания ответа сервера (в секундах).	—	60
Не возвращать более чем	Максимальное количество записей за один запрос.	Любое число (0 = без ограничения)	0
Постраничное получение результатов	Получение результатов частями.	Использовать / Отключить	Использовать
Размер страницы	Количество записей, возвращаемых за одну страницу при постраничном получении.	—	100
Фильтр поиска	Фильтр поиска учетных записей в LDAP.	По умолчанию / Настраиваемый	По умолчанию
База поиска	DN контейнера, где выполняется поиск.	Любой DN	Автоопределение
Получение контактов	Определяет, какие контакты сохраняются локально.	Скачать все / Сохранять последние / Не хранить	Скачать все
Автообновление каталога	Настройка синхронизации данных с сервером.	Никогда / 1 раз в день / Раз в 60 мин / Раз в 30 мин	Никогда

Редактирование книги LDAP

1. Перейдите в раздел **Контакты**.
2. Откройте окно со списком адресных книг. Для этого нажмите на название активной адресной книги в верхнем правом углу окна.
3. Наведите курсор на панель с профилем, настройки которого необходимо отредактировать.
4. Нажмите на кнопку **Настройки** .
5. Откроется окно с предпросмотром настроек.
6. Нажмите на кнопку **Редактировать** .



7. Откроется форма для редактирования настроек адресной книги.
8. Внесите изменения и нажмите кнопку **Сохранить**.

Удаление книги LDAP

1. Перейдите в раздел **Контакты**.
2. Откройте окно со списком адресных книг. Для этого нажмите на название активной адресной книги в верхнем правом углу окна.
3. Наведите курсор на панель с профилем, настройки которого необходимо отредактировать.
4. Нажмите на кнопку **Настройки** .
5. Откроется окно с предпросмотром настроек.
6. Нажмите на кнопку **Удалить** .
7. Подтвердите действие в модальном окне.

Адресная книга удаляется. Удаляются все ее контакты.

Возможные ошибки

При возникновении ошибки вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Описание	Рекомендуемые действия
Не удалось подключиться к LDAP	Возможно, указаны некорректные параметры подключения	Проверьте правильность заполнения данных

Инструкции по теме

- Создание локального контакта
- Добавление адресной книги ALD Pro
- Действия с локальными контактами
- Добавление адресной книги CardDAV

Открыть статью на сайте

Адресная книга ALD Pro

- Основные понятия
- Добавление книги ALD Pro
- Редактирование книги ALD Pro
- Удаление книги ALD Pro
- Возможные ошибки

Основные понятия

В КриптоАРМ поддерживается импорт контактов и синхронизации информации о них из адресной книги ALD Pro.

ALD Pro — это служба каталога для Linux, программный комплекс централизованного управления компьютерами с помощью групповых политик, а также прикладными сервисами для ИТ-инфраструктур организаций различного масштаба.

Принцип работы

1. КриптоАРМ подключается к серверу ALD Pro с использованием учетной записи пользователя, предназначенной для чтения каталога.
2. По заданной базе поиска и фильтру извлекаются контакты.
3. Полученные записи отображаются в интерфейсе КриптоАРМ как отдельная адресная книга.
4. При включенном автообновлении изменения на сервере автоматически отражаются в КриптоАРМ.

> 💡 Адресная книга ALD Pro не заменяет локальные контакты, а дополняет их. Можно использовать несколько адресных книг одновременно и комбинировать их с локальными контактами.

Добавление книги ALD Pro

Шаг 1. Настройка ALD Pro

1. Создайте в ALD Pro учетную запись, с которой будет выполняться подключение к серверу.
2. Настройте фильтры. В зависимости от настроек клиента, могут использоваться фильтры, в которых можно отсечь ненужные записи.

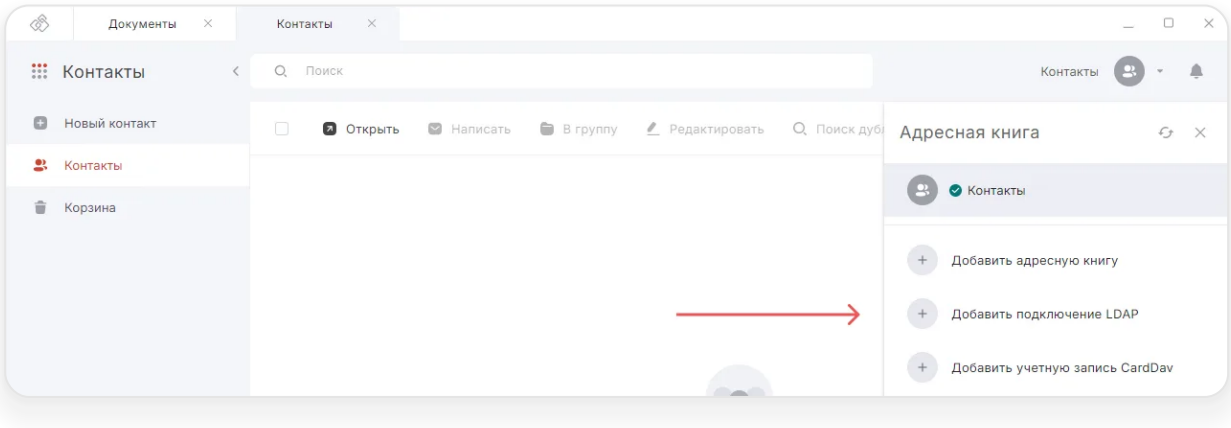
3. Сервер ALD Pro должен быть доступен по сети с компьютера, на котором работает почтовый клиент. Если данный сервер находится за NAT или он закрыт брандмауэром, то необходимо обеспечить доступ по следующим портам:

   - 389 tcp или udp. Незащищенный доступ к активному каталогу.
   - 636 tcp или udp. Доступ с защитой SSL.

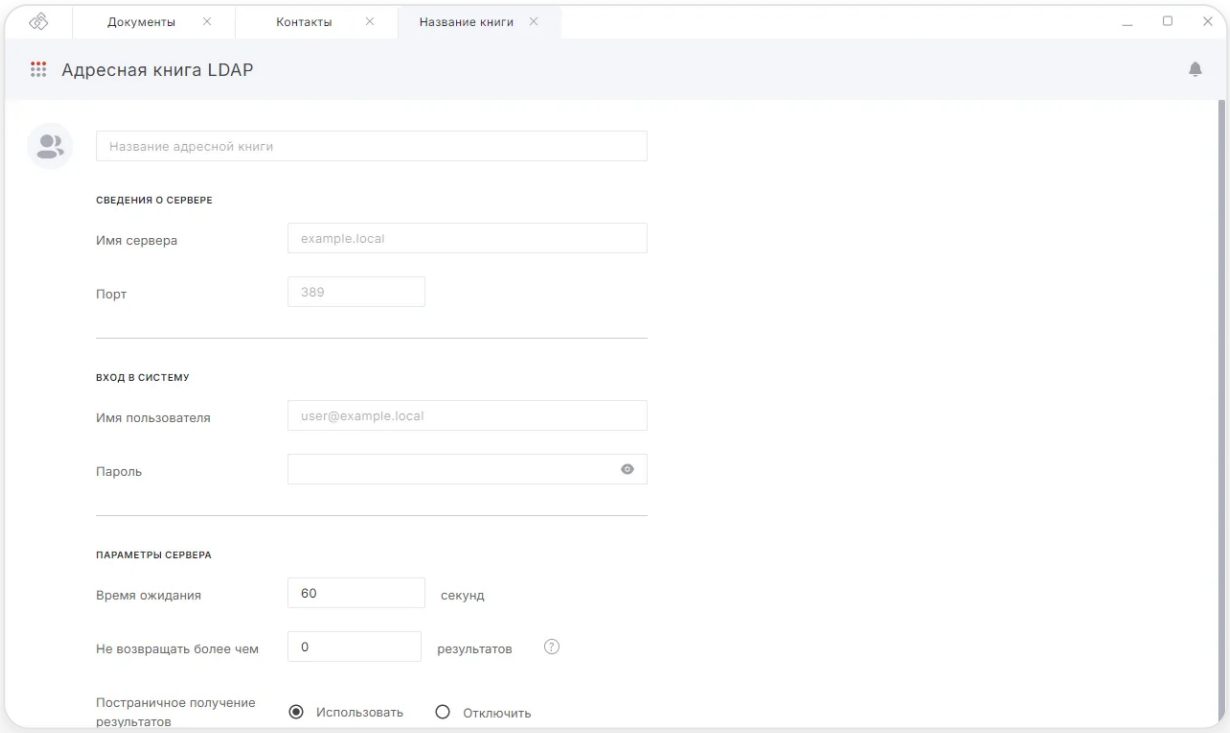
   Достаточно открыть и использовать один из данных портов, желательно 636.

Шаг 2. Создание подключения в КриптоАРМ

1. Перейдите в раздел **Контакты**.
2. Откройте окно со списком адресных книг. Для этого нажмите на название активной адресной книги в верхнем правом углу окна.
3. Выберите **Добавить подключение LDAP**.



4. Откроется форма добавления адресной книги.



5. Укажите настройки подключения.

6. Нажмите **Сохранить**.

После подключения появится новая адресная книга. Чтобы увидеть её контакты, переключитесь на неё.

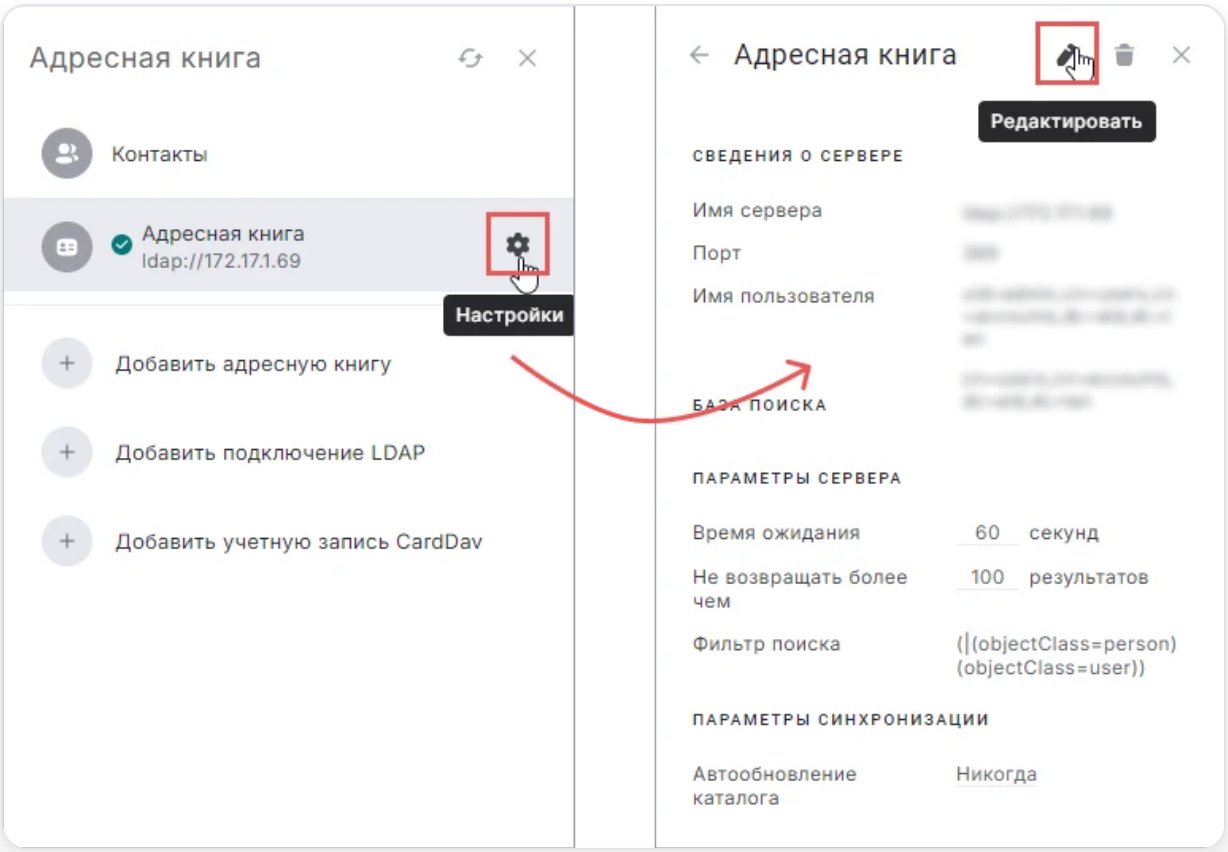
Описание параметров подключения

Название поля	Описание	Варианты выбора	По умолчанию
Название адресной книги	Имя книги, отображаемое в приложении.	Любое текстовое	—
Имя сервера	Адрес LDAP-сервера для подключения.	IP-адрес или доменное имя	—
Порт	Порт для подключения к LDAP-серверу.	—	—
Имя пользователя	Учетная запись для подключения к серверу.	—	—
Пароль	Пароль для указанной учетной записи.	—	—
Время ожидания	Время ожидания ответа сервера (в секундах).	—	60

Название поля	Описание	Варианты выбора	По умолчанию
Не возвращать более чем	Максимальное количество записей за один запрос.	Любое число (0 = без ограничения)	0
Постраничное получение результатов	Получение результатов частями.	Использовать / Отключить	Использовать
Размер страницы	Количество записей, возвращаемых за одну страницу при постраничном получении.	—	100
Фильтр поиска	Фильтр поиска учетных записей в LDAP.	По умолчанию / Настраиваемый	По умолчанию
База поиска	DN контейнера, где выполняется поиск.	Любой DN	Автоопределение
Получение контактов	Определяет, какие контакты сохраняются локально.	Скачать все / Сохранять последние / Не хранить	Скачать все
Автообновление каталога	Настройка синхронизации данных с сервером.	Никогда / 1 раз в день / Раз в 60 мин / Раз в 30 мин	Никогда

Редактирование книги ALD Pro

1. Перейдите в раздел **Контакты**.
2. Откройте окно со списком адресных книг. Для этого нажмите на название активной адресной книги в верхнем правом углу окна.
3. Наведите курсор на панель с профилем, настройки которого необходимо отредактировать.
4. Нажмите на кнопку **Настройки** .
5. Откроется окно с предпросмотром настроек.
6. Нажмите на кнопку **Редактировать** .



7. Откроется форма для редактирования настроек адресной книги.
8. Внесите изменения и нажмите кнопку **Сохранить**.

Удаление книги ALD Pro

1. Перейдите в раздел **Контакты**.
2. Откройте окно со списком адресных книг. Для этого нажмите на название активной адресной книги в верхнем правом углу окна.
3. Наведите курсор на панель с профилем, настройки которого необходимо отредактировать.
4. Нажмите на кнопку **Настройки** .
5. Откроется окно с предпросмотром настроек.
6. Нажмите на кнопку **Удалить** .
7. Подтвердите действие в модальном окне.

Возможные ошибки

При возникновении ошибки вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Описание	Рекомендуемые действия
Не удалось подключиться к ALD Pro	Возможно, указаны некорректные параметры подключения	Проверьте правильность заполнения данных

Инструкции по теме

- Создание локального контакта
- Действия с локальными контактами
- Настройка аватаров
- Добавление адресной книги LDAP
- Добавление адресной книги CardDAV

Открыть статью на сайте

Адресная книга CardDAV

- Основные понятия
- Добавление книги CardDAV
- Редактирование книги CardDAV
- Удаление книги CardDAV
- Возможные ошибки

Основные понятия

CardDAV — это открытый интернет-протокол для синхронизации и управления контактами, основанный на стандарте vCard. Протокол обеспечивает централизованное хранение контактной информации на сервере и её доступ с различных устройств и приложений.

Принцип работы

1. **Подключение к серверу**: КриптоАРМ использует учетную запись пользователя для доступа к серверу CardDAV.
2. **Получение контактов**: приложение получает список контактов в формате vCard и отображает их в интерфейсе.
3. **Синхронизация**: изменения, внесённые локально или на сервере, синхронизируются по выбранному интервалу и направлению.
4. **Двусторонняя или односторонняя синхронизация**: данные могут синхронизироваться в обе стороны (локально ↔ сервер) или только с сервера на локальное устройство.

> 💡 CardDAV работает поверх защищённого соединения HTTPS, что обеспечивает безопасную передачу данных между клиентом и сервером.

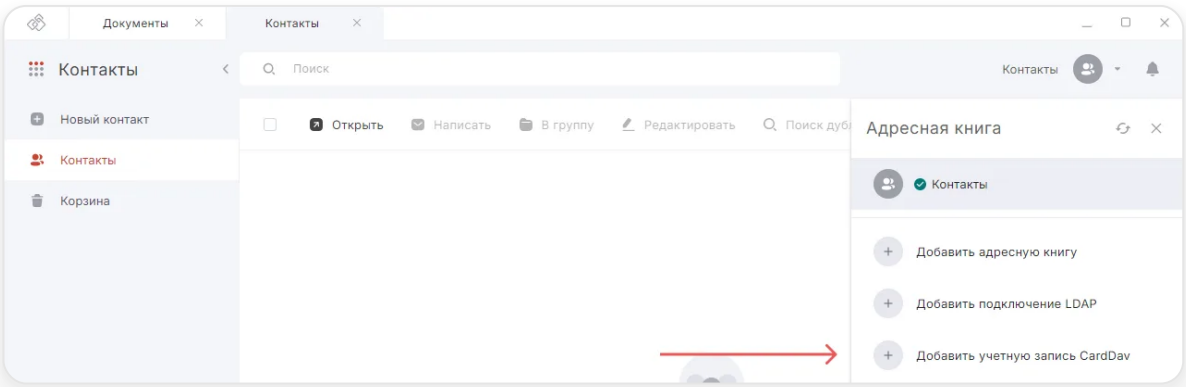
Добавление книги CardDAV

Шаг 1. Создание пароля

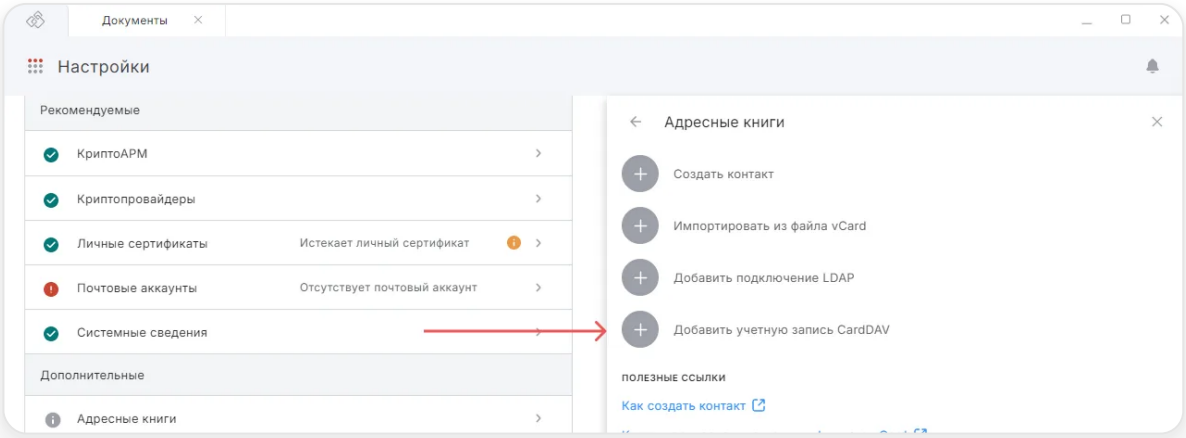
В качестве пароля может выступать обычный пароль или специальный пароль приложения, который необходимо создать в настройках сервиса, на котором размещена адресная книга.

Шаг 2. Создание подключения в КриптоАРМ

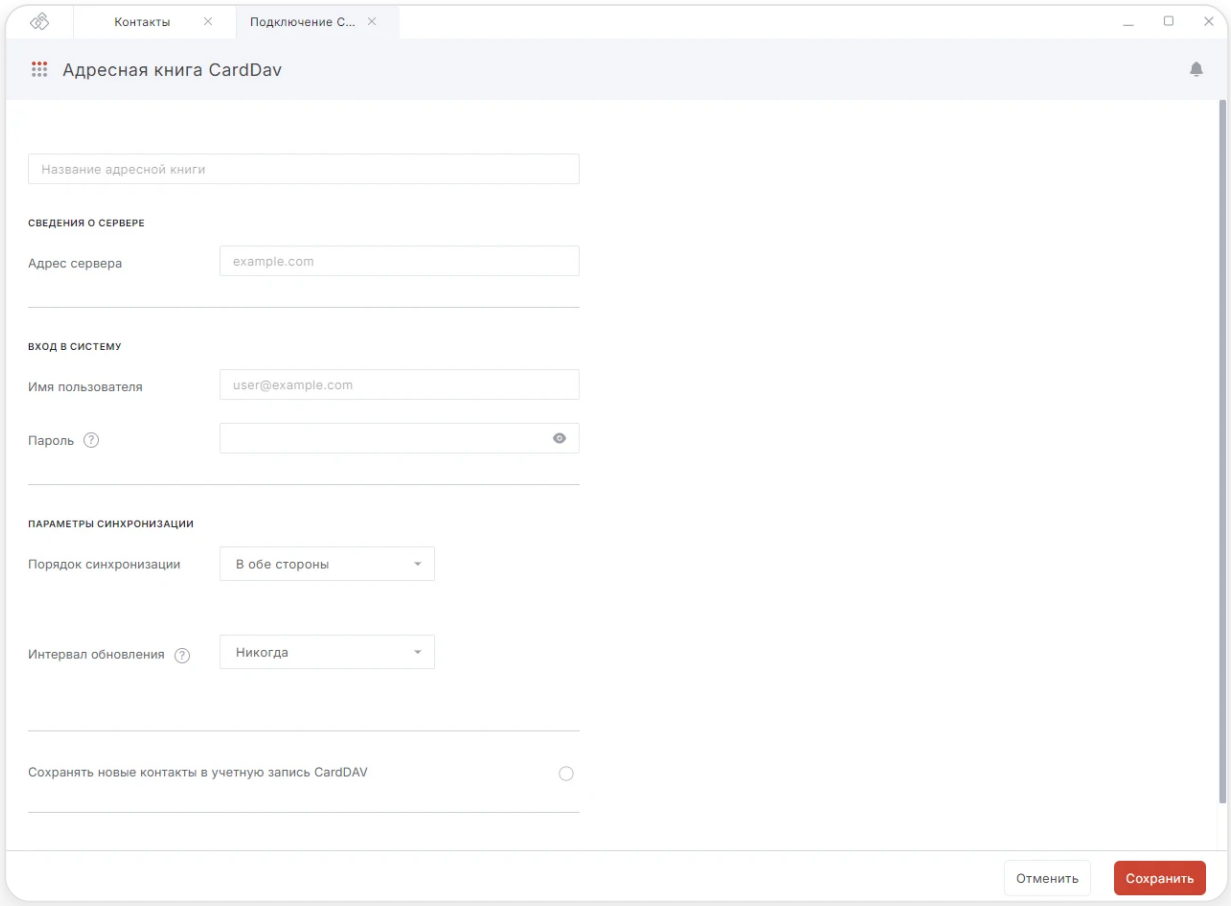
1. Откройте форму подключения:
   - Перейдите в раздел **Контакты**. Откройте окно со списком адресных книг. Для этого нажмите на название активной адресной книги в верхнем правом углу окна. Выберите действие **Добавить учётную запись CardDAV**.



   - Перейдите в раздел **Настройки** → проверка **Адресные книги**. Нажмите на кнопку **Добавить** в верхней части окна и выберите действие **Добавить учётную запись CardDAV**.



2. Откроется форма добавления адресной книги.



3. Укажите настройки подключения.

4. Нажмите **Сохранить**.

После подключения появится новая адресная книга. Чтобы увидеть её контакты, переключитесь на неё.

Описание параметров подключения

Название поля	Описание
Название адресной книги	Произвольное название, которое будет отображаться в приложении
Адрес сервера	Адрес сервера, на котором размещена книга
Имя пользователя	Учетная запись для подключения к серверу
Пароль	Пароль для учетной записи
Интервал обновления	Частота синхронизации адресной книги с почтовым сервисом. По умолчанию «Никогда»
Порядок синхронизации	По умолчанию выставлено значение «В обе стороны»

Название поля	Описание
Сохранять новые контакты в учетную запись CardDAV	По умолчанию настройка неактивна

Редактирование книги CardDAV

1. Перейдите в раздел **Контакты**.
2. Откройте окно со списком адресных книг. Для этого нажмите на название активной адресной книги в верхнем правом углу окна.
3. Наведите курсор на панель с профилем, настройки которого необходимо отредактировать.
4. Нажмите на кнопку **Настройки** .
5. Откроется окно с предпросмотром настроек.
6. Нажмите на кнопку **Редактировать** .
7. Откроется форма для редактирования настроек адресной книги.
8. Внесите изменения и нажмите кнопку **Сохранить**.

Удаление книги CardDAV

1. Перейдите в раздел **Контакты**.
2. Откройте окно со списком адресных книг. Для этого нажмите на название активной адресной книги в верхнем правом углу окна.
3. Наведите курсор на панель с профилем, настройки которого необходимо отредактировать.
4. Нажмите на кнопку **Настройки** .
5. Откроется окно с предпросмотром настроек.
6. Нажмите на кнопку **Удалить** .
7. Подтвердите действие в модальном окне.

Возможные ошибки

При возникновении ошибки вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Описание	Рекомендуемые действия
Ошибка синхронизации аккаунта CardDAV	Возможно, указаны некорректные параметры подключения	Проверьте правильность заполнения данных
Ошибка получения контактов		

Ошибка	Описание	Рекомендуемые действия
	Возможно, указаны некорректные параметры подключения, либо отсутствует подключение к сети Интернет	1. Проверьте подключение к сети Интернет, 2. Проверьте правильность заполнения данных.

Инструкции по теме

- Создание локального контакта
- Действия с локальными контактами
- Настройка аватаров
- Добавление адресной книги LDAP
- Добавление адресной книги ALD Pro

Открыть статью на сайте

Импорт контактов vCard

- Основные понятия
- Импорт контактов
- Возможные ошибки

Основные понятия

vCard (Virtual Contact File) — международный стандарт обмена электронными визитными карточками, предназначенный для хранения и передачи информации о контактах. Формат vCard широко используется в почтовых клиентах, мобильных устройствах, CRM-системах и корпоративных каталогах.

Формат поддерживает хранение различных данных о контакте, включая:

- контактную информацию (ФИО, номера телефонов, e-mail-адреса),
- адресные и демографические данные (место работы, адрес, дата рождения),
- мультимедийные элементы (фотографии, логотипы),
- сертификаты для безопасного обмена документами и письмами.

Принцип работы

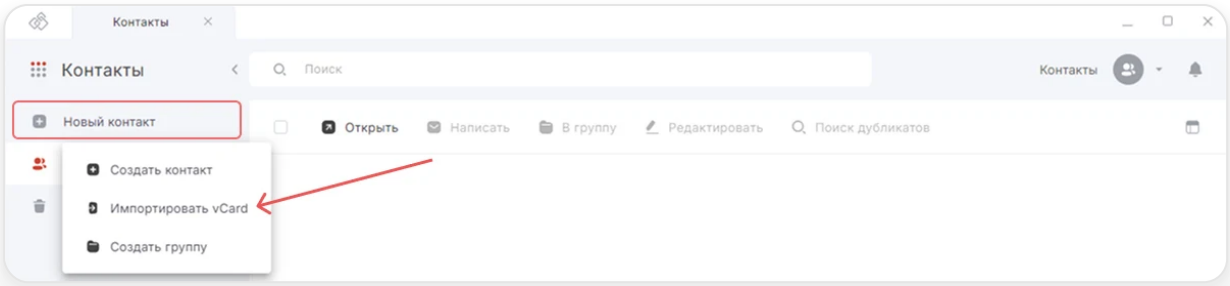
1. Пользователь выбирает файл vCard для импорта.
2. Программа считывает все контакты и извлекает атрибуты (ФИО, телефон, email, и др.).
3. Контакты импортируются в выбранную адресную книгу и при необходимости в заданную группу.
4. При успешном завершении отображается уведомление с количеством импортированных контактов.

> 💡 Формат vCard позволяет повторно использовать одни и те же данные в разных приложениях, а также синхронизировать их с корпоративными каталогами и мобильными устройствами.

Импорт контактов

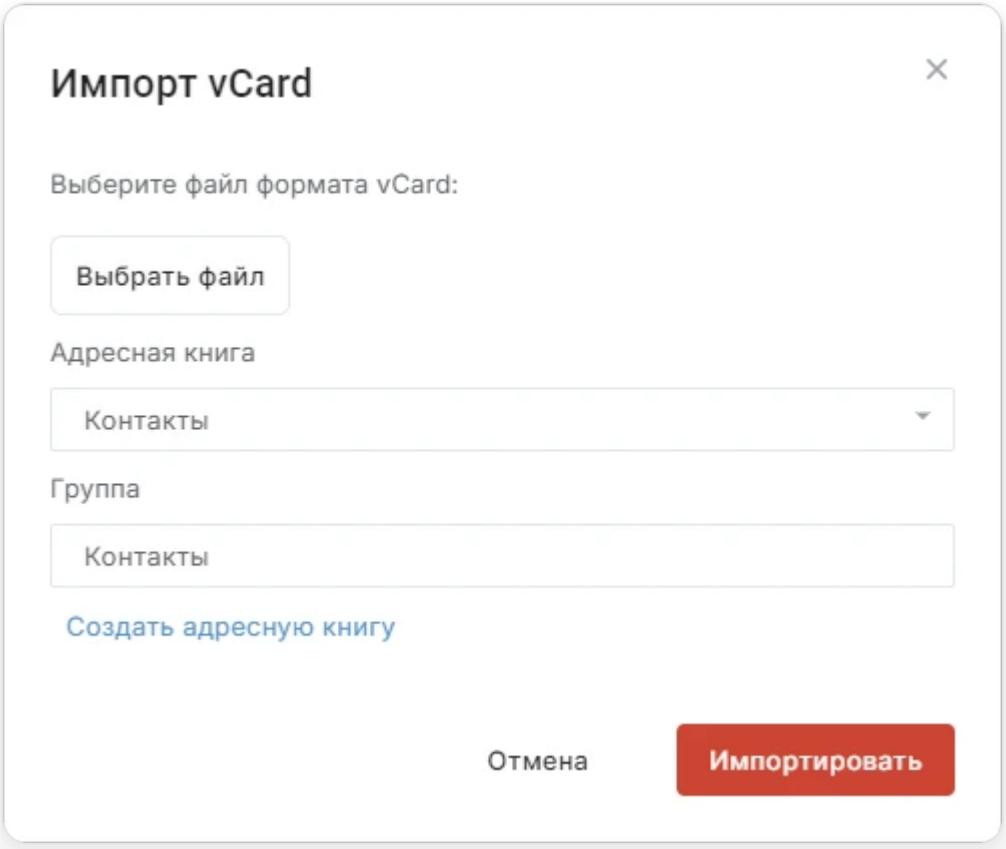
Способ 1: из раздела "Контакты"

1. Перейдите в раздел **Контакты**.
2. Нажмите на кнопку **Новый контакт** в боковом меню.
3. В появившемся меню выберите **Импорт vCard**.

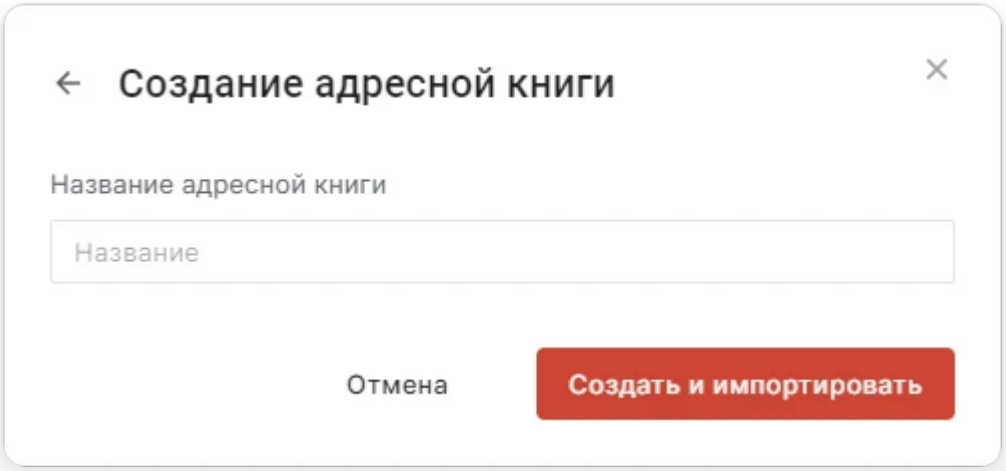


4. Откроется окно **Импорт vCard**.

   - Нажмите **Выбрать файл** и в появившемся окне файлового менеджера укажите путь к файлу с контактами.
   - Выберите адресную книгу, в которую необходимо импортировать контакты.
   - Укажите группу, в которую будут вложены контакты.



   - При необходимости создайте новую группу в указанной адресной книге.



5. Нажмите **Импортировать**.

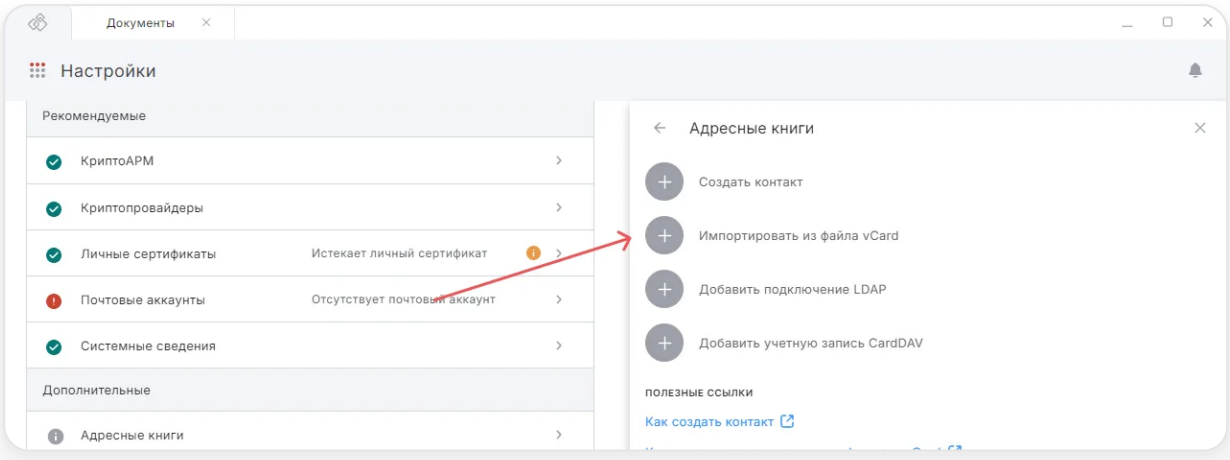
Будет запущен процесс импорта.

После окончания операции будет выведено уведомление с количеством импортированных контактов.

> 💡 Если экспортируется большой объём контактов, операция может занять некоторое время.

Способ 2: из раздела "Настройки"

1. Перейдите в раздел **Настройки** → проверка **Адресные книги**.
2. Откроется окно со списком адресных книг (если они обнаружены).
3. Нажмите на кнопку **Добавить** в верхней части окна.
4. Выберите действие **Импортировать из файла vCard**.



5. Откроется окно **Импорт vCard**.

6. Следуйте шагам из инструкции Способ 1: из раздела "Контакты".

Возможные ошибки

При возникновении ошибки вы увидите уведомление в правом верхнем углу. Для детального анализа откройте список уведомлений и перейдите в Журнал.

Ошибка	Описание	Рекомендуемые действия
Не удалось импортировать контакты	Возможно, файл пустой или поврежден	Проверьте содержимое файла и повторите импорт

Инструкции по теме

- Создание локального контакта
- Действия с локальными контактами
- Настройка аватаров
- Добавление адресной книги LDAP
- Добавление адресной книги ALD Pro

Открыть статью на сайте

Центр уведомлений

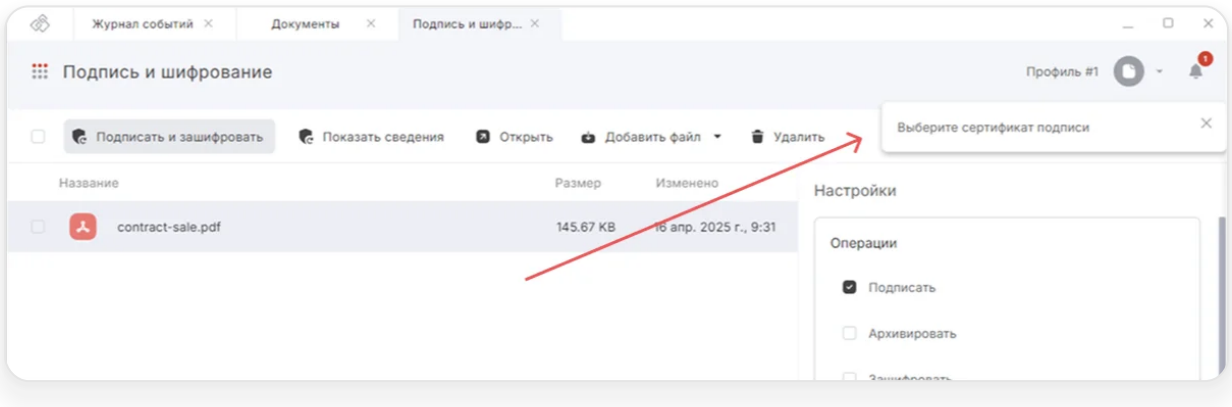
- Принципы работы уведомлений
- Управление уведомлениями

Принципы работы уведомлений

Приложение использует многоуровневую систему оповещений о событиях и ошибках:

1. Всплывающие уведомления

- **Расположение**: верхний правый угол интерфейса,
- **Длительность показа**: 5 секунд,
- **Содержание**: Краткое описание события/ошибки.



2. Центр уведомлений

Открывается одним из способов:

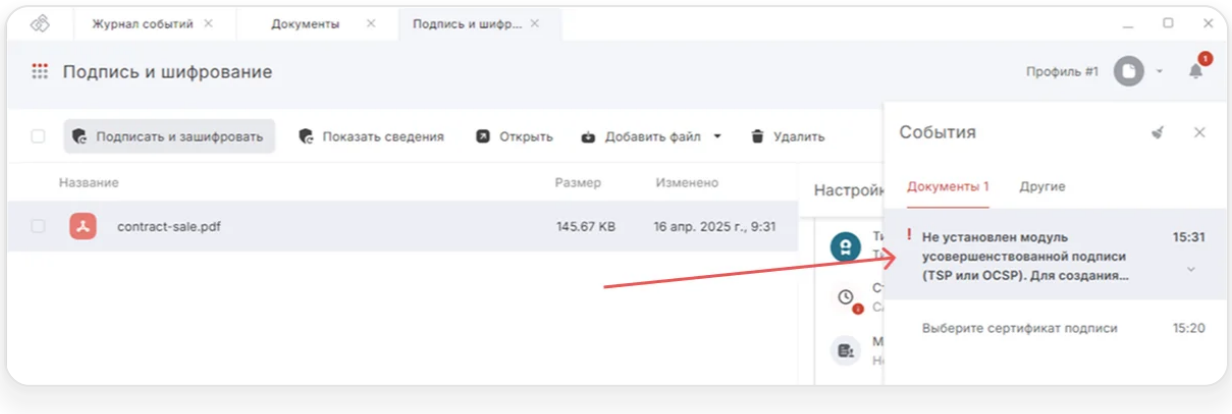
- Клик по всплывающему уведомлению,
- Нажатие на иконку  с индикатором новых событий.

Структура центра уведомлений:

Вкладка	Содержание
Текущая	События, относящиеся к активному разделу
Другие	Все остальные системные уведомления

Особенности отображения:

- Новые уведомления выделены **жирным шрифтом**



- Сортировка по времени (новые сверху)

Управление уведомлениями

1. **Просмотр деталей**:
    - Нажмите на уведомление для раскрытия дополнительной информации,
    - Используйте кнопку **Перейти в журнал** для полного отчета.
2. **Очистка**:
    - Удалите все уведомления с помощью кнопки

Открыть статью на сайте

Журнал событий

- Назначение
- Как открыть журнал
- Классификация событий
- Работа с записями журнала
- Настройки журнала
- Загрузка архивного журнала
- Просмотр расположения файла событий
- Фильтрация и поиск

Назначение

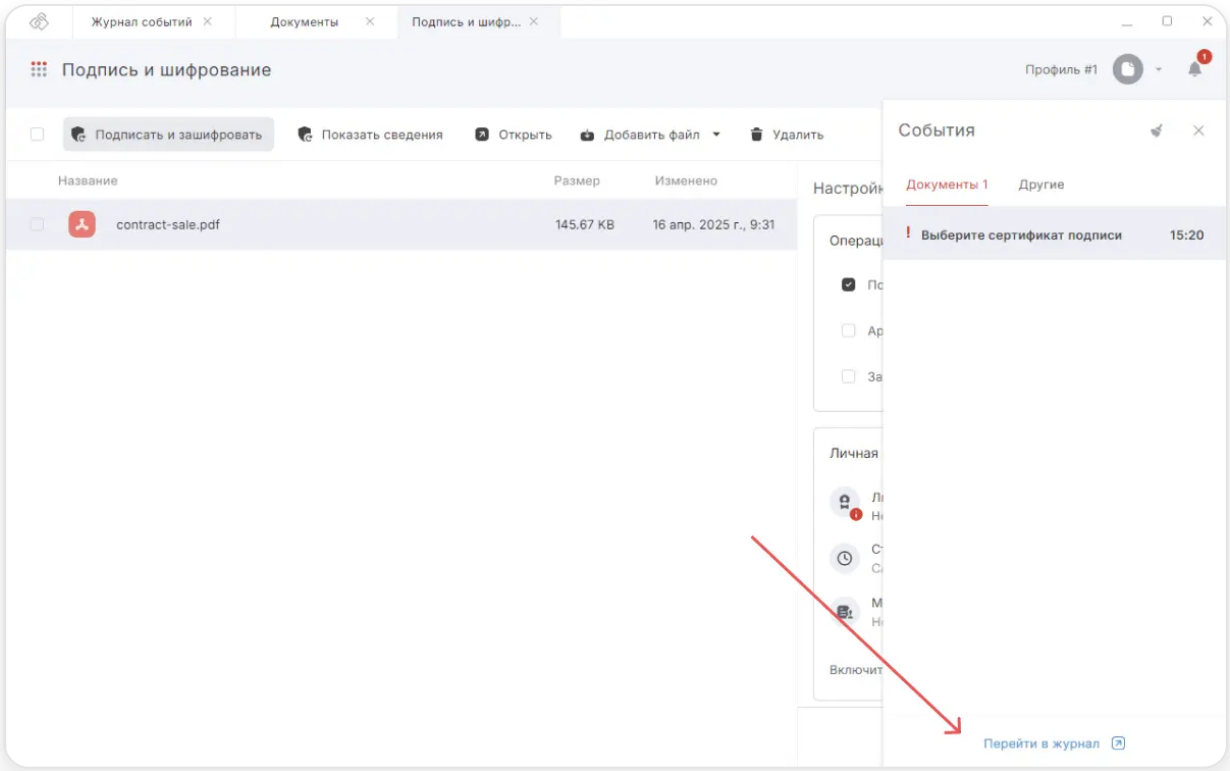
Журнал событий фиксирует все значимые действия и ошибки в приложении, предоставляя:

- Детальную информацию о выполненных операциях
- Диагностические данные для устранения неполадок
- Историю работы для аудита и анализа

Как открыть журнал

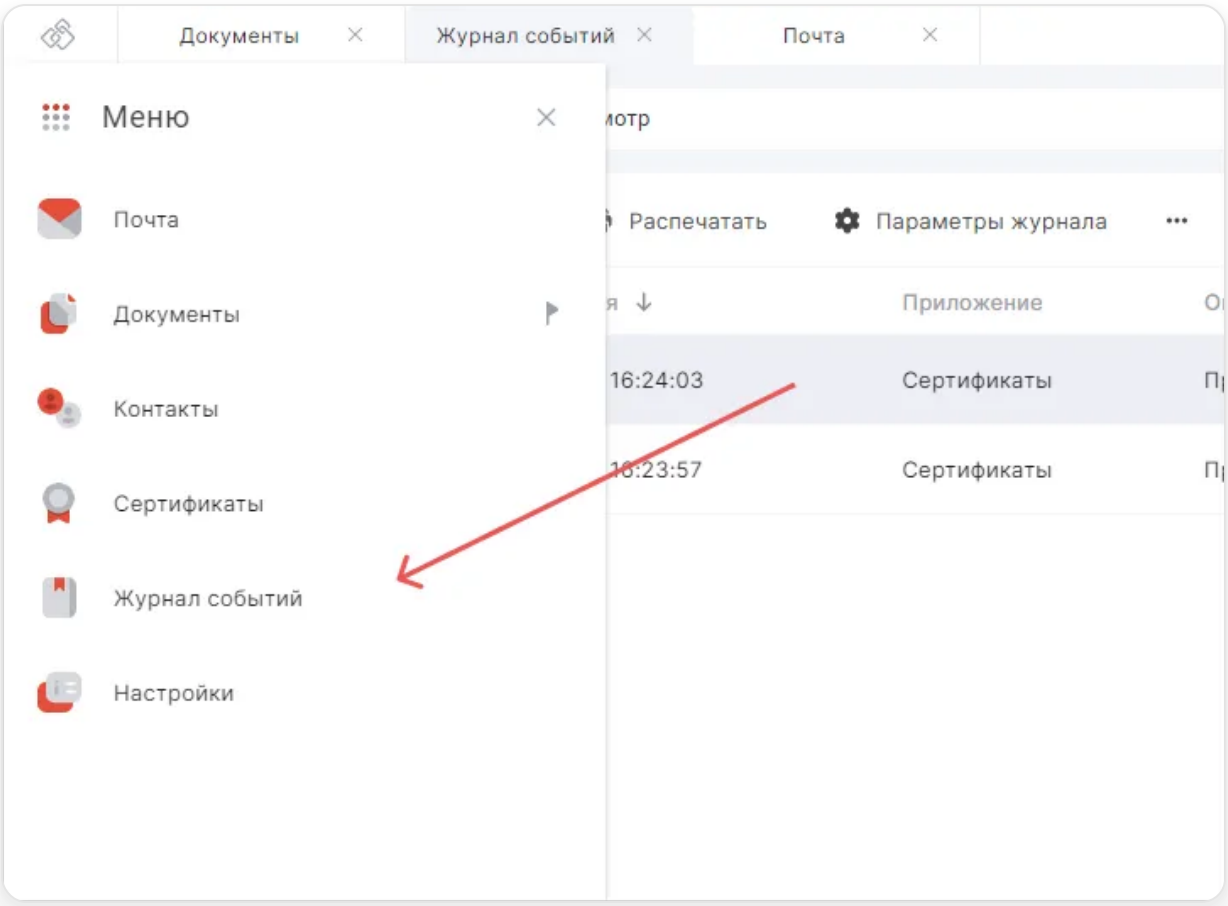
Способ 1: Через центр уведомлений

1. Откройте центр уведомлений по кнопке , размещенной в верхнем правом углу окна.
2. Нажмите на **Перейти в журнал**.



Способ 2: Через главное меню

1. Откройте главное меню приложения.
2. Выберите раздел **Журнал**.



Классификация событий

Тип	Иконка	Описание	Примеры
Ошибка		Критические сбои	Не удалось подписать документ
Информация		Штатные операции	Успешная синхронизация

Работа с записями журнала

1. Просмотр деталей

1. Выделите запись в списке.
2. Нажмите на кнопку **Подробно** на панели действий.
3. В области справа от списка отобразится подробная информация о событии.

2. Копирование информации

1. Откройте детали события.
2. Нажмите **Скопировать** .
3. Данные будут сохранены в буфер обмена.

3. Экспорт в файл

1. Выделите с помощью флагов нужные события.
2. Нажмите на кнопку **Сохранить** на панели действий.
3. В файловом менеджере задайте имя и расположение файла .log.

4. Отправка по email

1. Выделите события
2. Нажмите **Отправить** на панели действий.
3. Будет создано новое письмо с вложенным файлом журнала.

5. Печать событий

1. Выделите с помощью флагов нужные события.
2. На верхней панели действий нажмите на кнопку **Распечатать**.

Настройки журнала

В программе можно настроить размер журнала и уровни логирования:

1. На панели действий нажмите на кнопку **Параметры журнала**.
2. Задайте параметры журнала:
    - Размер журнала (по умолчанию 2 МБ),
    - Уровень логирования.

> ⚠️ **Обратите внимание**:
> - Максимальный размер журнала — 10 МБ. При достижении максимального размера файла создается новый журнал без перезаписи старого.
> - Общие параметры, такие как имя, расположение, даты создания и изменения, недоступны для редактирования и являются информационными.

3. Нажмите на кнопку **Сохранить**.

Загрузка архивного журнала

Чтобы посмотреть события из архивного журнала:

1. На панели действий нажмите на кнопку **Загрузить архив**.
2. Укажите путь к файлу с архивным журналом.

Архивная копия открывается в новой вкладке.

Просмотр расположения файла событий

Чтобы перейти к расположению файла событий, нажмите на кнопку **Показать в папке** на панели действий.

Фильтрация и поиск

Быстрый поиск

Для фильтрации журнала используется строка поиска.

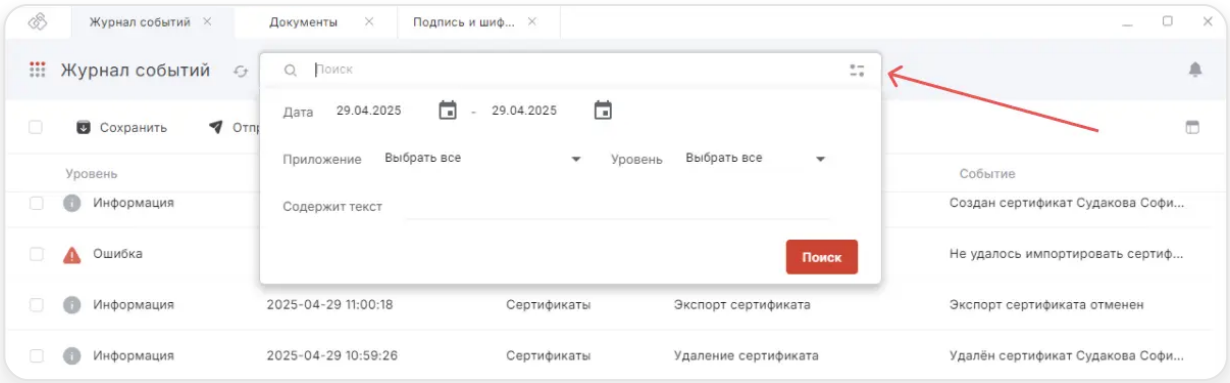
1. Установите курсор в строку поиска.
2. Введите поисковую фразу.

Поиск осуществляется по названию операции и тексту события.

Расширенная фильтрация

Для более детальной фильтрации вы можете задать параметры.

1. Нажмите на кнопку **Открыть фильтр** в строке поиска.
2. Укажите параметры:
   - **Дата** — диапазон дат;
   - **Приложение** — раздел, в котором возникло событие;
   - **Уровень логирования**;
   - **Содержит текст** — ключевые слова в сообщении.



3. Нажмите кнопку **Поиск**.

Чтобы отменить примененный фильтр, нажмите на кнопку **Отменить запрос** ✕ в строке поиска.

Открыть статью на сайте

Часто задаваемые вопросы

О продукте

- Возможности КриптоАРМ
- Какие криптопровайдеры поддерживаются
- Какие типы ключевых носителей поддерживаются
- Какие системные требования нужны
- Отправка отзыва о КриптоАРМ
- Определение установленной версии КриптоАРМ
- Изменение раздела при запуске

Начало работы

- Скачать и установить КриптоАРМ на Windows
- Скачать и установить КриптоАРМ на Linux
- Скачать и установить КриптоАРМ на macOS
- Скачать и установить КриптоПро CSP на Windows
- Скачать и установить КриптоПро CSP на Linux
- Скачать и установить КриптоПро CSP на macOS
- Установка сертификата из ключевого контейнера
- Установка сертификата из файла .pfx
- Установка сертификат из DSS
- Создание самоподписанного сертификата
- Получение квалифицированной электронной подписи
- Установка корневого или промежуточного сертификатов
- Установка сертификата другого пользователя

Лицензирование

- Как узнать статус лицензии КриптоАРМ
- Как узнать статус лицензии КриптоПро CSP
- Ввод лицензионного ключа КриптоАРМ
- Ввод лицензионного ключа КриптоПро CSP

Проверка рабочего места

- Запуск проверки рабочего места
- Скачивание или отправка отчета о системе

Подпись и шифрование

- Подпись файла со стандартом CAdES
- Подпись файла со стандартом PAdES
- Установка подписи в размеченную область
- Подпись pdf-файла сертифицирующей подписью
- Создание печатной формы со штампом для pdf-файлов
- Шифрование файла

Проверка и расшифрование

- Расшифрование файла
- Проверка подписи файла
- Снятие подписи с файла

МЧД

- Просмотр визуализации МЧД
- Печать МЧД
- Проверка статуса МЧД

Почтовые настройки

- Как добавить почтовый аккаунт:
  - почта Mail,
  - Яндекс почта,
  - Gmail,
  - Outlook,
  - iCloud,
  - Rambler.
- Открытие настройки аккаунта
- Изменение пароля в аккаунте
- Настройка подписи и шифрования исходящих писем
- Привязка сертификата подписи к аккаунту
- Создание подписи (в конце письма)
- Настройка отображения информации о сертификате в подписи (в конце письма)
- Настройка автоответчика
- Настройка пересылки писем в другой ящик

Адресные книги

- Подключение адресной книги LDAP
- Подключение адресной книги ALDPro
- Добавление адресной книги по протоколу CardDAV

Работа с письмами

- Отправка подписанного и зашифрованного письма
- Отправка письма с уведомлением о доставке и прочтении
- Проверка подписи письма
- Расшифрование письма
- Как узнать доставлено ли письмо
- Как узнать прочитано ли письмо
- Открытие письма в формате .eml
- Расшифрование письма в формате.p7m
- Проверка подписи письма с вложением smime.p7s

Открыть статью на сайте

Глоссарий

- Сертификаты
- Подпись и шифрование
- Почта

Сертификаты

Сертификат электронной подписи

Электронный документ, который подтверждает владение ключом электронной подписи

Сертификат усиленной квалифицированной электронной подписи (УКЭП)

Выпускает только аккредитованный удостоверяющий центр. Документ, подписанный УКЭП, действителен для любой организации или ведомства.

Самоподписанный сертификат

Сертификат, изданный самим пользователем, без обращения к Удостоверяющему центру.

Открытый ключ электронной подписи

Ключ проверки электронной подписи. Содержит содержит уникальный код, с помощью которого можно проверить подлинность электронной подписи. Сертификат открытого ключа содержит сведения о подписанте (ФИО, СНИЛС и др.), об удостоверяющем центре, который выдал ЭП и срок действия ключа.

Закрытый ключ электронной подписи

Секретный уникальный набор символов, который также формируется криптопровайдером. Закрытый ключ необходим для формирования электронной подписи и хранится в зашифрованном виде, как правило, на носителе (токене). Доступ к закрытому ключу имеет только владелец.

Запрос на сертификат

Электронный документ, который содержит информацию для получения сертификата электронной подписи в Удостоверяющем центре

Ключевой контейнер

Способ хранения закрытых ключей. Кроме ключей, он содержит служебную информацию, необходимую для обеспечения криптографической защиты ключей, их целостности и т.п. Физическое представление ключевого контейнера зависит от типа ключевого носителя: флешка, жёсткий диск, смарт-карты, реестр.

Статус сертификата электронной подписи

Информация о действительности сертификата

Удостоверяющий центр (УЦ)

Доверенная организация, которая имеет право выпускать сертификаты электронной подписи (ЭП) юридическим и физическим лицам

Корневой сертификат

Цифровой документ, в котором содержится информация об удостоверяющем центре. Корневые сертификаты выдаются только организациям и могут иметь разный уровень. В Российской Федерации главный корневой сертификат принадлежит Министерству цифрового развития. На основе этого сертификата Минцифры РФ выдаёт удостоверяющим центрам собственные сертификаты, подписывая их своим корневым сертификатом.

Промежуточный сертификат

Сертификат, выданный удостоверяющим центрам

Сертификат другого пользователя

Сертификат, принадлежащий другому пользователю. Предназначен для шифрования документов в его адрес.

Список отзыва сертификатов

Список сертификатов, которые удостоверяющий центр пометил как отозванные.

Цепочка сертификации или цепочка доверия

Иерархическая коллекция сертификатов. Для квалифицированных сертификатов ЭП, как правило, состоит из 3 звеньев. Верхнее звено - корневой сертификат. Среднее звено - сертификат удостоверяющего центра. Конечное звено - сертификат пользователя.

Сервис DSS

Сервис электронной подписи. Предназначен для шифрования и расшифрования электронных документов, формирования запросов на создание и управление сертификатами ключей проверки электронной подписи, создания и проверки электронной подписи различного формата криптографических сообщений.

Подпись и шифрование

Электронная подпись (ЭП)

Информация в электронно-цифровой форме для определения и подтверждения личности автора подписи

Усиленная неквалифицированная электронная подпись (УНЭП)

Цифровой аналог собственноручной подписи. Применяется, если стороны заключили соглашение об этом или так указано в законе. В таких случаях документы, подписанные от руки или с помощью УНЭП, имеют равную юридическую силу.

Усиленная квалифицированная электронная подпись (УКЭП)

Цифровой аналог собственноручной подписи. Ей можно подписывать любые документы без предварительной договорённости с другой стороной.

Профили подписи в КриптоАРМ

Заранее подготовленные наборы настроек, которые можно применять для выполнения подписи, архивирования и шифрования.

Алгоритмы подписи

Криптографические алгоритмы, которые используются для создания электронной цифровой подписи

Алгоритмы шифрования

Криптографические алгоритмы, которые используются для шифрования файлов

Криптопровайдер

Провайдер криптографических услуг, криптопровайдер специализированный программный модуль или набор модулей, предоставляющих средства шифрования и дешифрования данных, цифровой подписи, а также генерации и хранения ключей.

Присоединенная подпись

Подпись, в процессе создания которой формируется специальный контейнер, в котором находятся как подписываемый документ, так и файл подписи.

Отсоединенная подпись

Файл подписи формируется и хранится отдельно от подписываемого документа.

Стандарт подписи CAdES-BES (Basic Electronic Signature)

Основной и простейший формат электронной подписи, описываемый в стандарте CAdES. Он обеспечивает базовую проверку подлинности данных и защиту их целостности

Стандарт подписи CAdES-T (Timestamp)

Формат электронной подписи, в которую автоматически добавляется штамп времени на подпись.

Стандарт подписи CAdES-X Long Type 1

Формат электронной подписи, включающий дополнительные атрибуты certificate-values и revocation-values, которые представляют собой полные данные сертификатов и списки отзыва сертификатов. А также штампы времени на подпись и ссылки на сертификаты и списки отзыва сертификатов.

Стандарт подписи CAdES-A (Archival)

Формат электронной подписи, сформированный на основе CAdES-X Long Type 1 или Type 2 путём добавления одного или нескольких атрибутов archive-time-stamp, представляющих собой архивные штампы времени.

Машиночитаемая доверенность

Аналог бумажной доверенности в электронном виде. Она создаётся в формате XML, который позволяет компьютеру прочитать её содержание и подтвердить личность того, кто подписал документ

Сертификация PDF документа

Позволяет защитить PDF документ от изменений путем его подписания электронной подписью, с указанием типа изменений, разрешенных для документа.

Конвертация PDF документа

При конвертации PDF документа происходит удаление скриптов, форм и прочих элементов, влияющих на безопасность и целостность документа.

Формат подписи CadES

Стандарт электронной подписи, представляющий собой расширенную версию стандарта электронной подписи CMS. Эту электронную подпись можно прикрепить к любому типу файла : текстовым файлам (.doc, .docx), электронным таблицам (.xls, .xlsx), изображениям (.jpg, .png, .gif) и PDF-файлам.

Формат подписи PadES

Формат, при котором подпись встраивается в PDF-документ. «Встроенная» подпись позволяет подписывать электронные документы без изменения формата файла и без создания отдельного файла подписи, как это происходит при использовании присоединенной и отсоединенной подписи соответственно. Подпись встраивается в электронный документ, и получатель может проверить документ на действительность электронной подписи.

Видимая подпись PDF документа

«Встроенная» подпись, которая отображается на странице документа в виде штампа.

Невидимая подпись PDF документа

«Встроенная» подпись, которая визуально на страницах не видна.

Область для штампа подписи в PDF документе

Область на странице PDF документа, размеченная для видимой подписи.

Произвольная область в PDF документе

Область для графического изображения или текста. В области можно разместить свой комментарий, статус или отметку о конфиденциальности документа.

Почта

Адрес электронной почты

Название электронного почтового ящика, который может получать (и отправлять) электронные письма в сети (например, в интернете или в локальной сети, не подключённой к интернету).

Почтовый сервер

Это программа, работающая у интернет-провайдеров и на крупных сайтах и используемая для передачи почты. Обычно пользователи не взаимодействуют с почтовыми серверами напрямую: электронная почта отправляется с помощью почтового клиента на почтовый сервер, который доставляет её в почтовый клиент получателя.

Почтовый клиент

Это программа (например, на компьютере или мобильном устройстве), которая используется для чтения и отправки электронных сообщений.

IMAP

Протокол, который используется для получения сообщений электронной почты с сервера. IMAP позволяет почтовым программам получать доступ не только к новым сообщениям, но и к папкам на сервере. Действия синхронизируются между несколькими почтовыми программами, подключёнными через IMAP.

POP

Протокол, который используется для получения сообщений электронной почты с сервера. В отличие от IMAP, POP позволяет почтовому клиенту загружать только последние сообщения, которыми можно управлять в клиенте и на устройстве.

SMTP

Протокол, который используется для передачи электронной почты. Он определяет формат сообщений и процедуру их передачи через Интернет от отправителя к получателю с помощью почтовых серверов.

S/MIME

Стандарт для шифрования и подписи электронных писем с помощью открытого ключа.

SSL

Протокол, который обеспечивает безопасное соединение между клиентом и сервером.

Логин (имя пользователя)

Имя почтового ящика — комбинация из букв и цифр, которая, как правило, находится в адресе перед именем домена.

Пароль

Набор символов, предназначенный для подтверждения личности.

Скрытая копия

Копия электронного письма, отправленного получателю, адрес электронной почты которого не указан (в качестве получателя) в сообщении

Копия

Копия электронного письма, отправленного получателю, адрес электронной почты которого указан в поле заголовка «Копия».

Тело письма

Основная часть электронного письма, которая содержит текст, изображения и другие данные (например, прикреплённые файлы).

LDAP

Протокол быстрого доступа к каталогам. Он позволяет получать и принимать через сеть данные из каталогов с иерархической структурой.

ALD Pro

Служба каталога для Linux, программный комплекс централизованного управления компьютерами с помощью групповых политик, а также прикладными сервисами для ИТ-инфраструктур организаций различного масштаба. Комплекс создан «Группой Астра».

CardDAV

Протокол адресной книги, предназначенный для предоставления пользователям доступа к данным на сервере.

vCard

текстовый формат для обмена электронными визитными карточками. В карточке может содержаться имя, номера телефонов, адрес электронной почты, адрес проживания, дата рождения, фотография, сертификат и другие данные контакта.

Gravatar

Сервис компании Automattic, позволяющий интернет-пользователям хранить свой аватар на специальном сервере.

Открыть статью на сайте

Описание API КриптоАРМ

- Общая информация
- Доступные команды
- Сценарий выполнения команд (для взаимодействия с web-приложениями)
- Сценарий выполнения команд (для взаимодействия с локальным приложением)
- Формат ссылки для web КриптоАРМ API
- Формат ссылки для локального варианта КриптоАРМ API
- Описание запросов и ответов

Общая информация

КриптоАРМ поддерживает API с двумя возможными точками вызова:

- Локальное приложение на рабочем месте,
- Web-приложение (сервис).

При вызове операции через API приложение КриптоАРМ будет запущено и отобразит необходимый раздел с переданными параметрами. Команду можно ввести через адресную строку браузера (вы можете размещать их так же, как ссылки на веб-страницы) или в терминале.

Для взаимодействия используется зарегистрированный протокол `cryptoarm://`.

Доступные команды

Команда	Описание
`signAndEncrypt`	выполнение криптографических операций над документами (подпись, шифрование, проверка подписи, расшифрование)
`certificates`	экспорт или импорт сертификатов, просмотр свойств сертификата
`certrequests`	генерация запросов на сертификат
`diagnostics`	диагностика рабочего места
`startView`	открыть окно или вкладку
`mail`	действия с электронными письмами

Сценарий выполнения команд (для взаимодействия с web-приложениями)

1. **Инициация операции**
    - Пользователь заходит на портал (веб-приложение).
    - Выбирает объекты (например, список документов) и действие (например, подпись).
2. **Генерация ссылки**
    - Портал формирует и отображает (или автоматически перенаправляет) ссылку с протоколом `cryptoarm://`, содержащую идентификатор операции.
3. **Запуск и запрос параметров**
    - Если КриптоАРМ не запущен, система автоматически его запускает.
    - КриптоАРМ обращается к порталу, запрашивая JSON с параметрами для выполнения операции.
    - JSON генерируется на сервере веб-приложения.
4. **Обработка команды**
    - Полученный JSON анализируется.
    - В зависимости от типа операции, КриптоАРМ может выполнить дополнительные запросы к веб-приложению (например, загрузка документов).
5. **Подтверждение пользователем**
    - Пользователь проверяет детали операции и подтверждает её выполнение.
    - На время выполнения функционал приложения блокируется для предотвращения конфликтов.
6. **Отправка результатов**
    - Результаты операции (например, подписанные документы) передаются обратно на сервер веб-приложения.

Сценарий выполнения команд (для взаимодействия с локальным приложением)

1. **Инициация операции**
    - Пользователь открывает стороннее приложение с поддержкой КриптоАРМ API.
    - Выбирает объекты (например, документы) и действие (например, подпись).

2. **Формирование JSON-запроса**
    - Приложение генерирует JSON-объект с параметрами операции и передаёт его в КриптоАРМ (через CLI или API).
3. **Запуск и обработка параметров**
    - Если КриптоАРМ не запущен, он автоматически стартует.
    - Приложение может дополнительно запросить JSON с сервера (если часть параметров хранится удалённо).
4. **Подтверждение пользователем**
    - Пользователь проверяет детали операции и подтверждает её выполнение.
    - Функционал приложения блокируется до завершения операции.
5. **Сохранение результатов**
    - Результаты (например, подписанные файлы) сохраняются в локальную папку, указанную в параметрах операции.

Формат ссылки для web КриптоАРМ API

```
cryptoarm://<command>/<URL>/?id=<id>
```

- `cryptoarm://` - зарегистрированный протокол
- `<command>` - выполняемая команда
- `<URL>` - ссылка на получение JSON с параметрами, нужными для выполнения команды
- `?id=<id>` - обязательный параметр. Идентификатор транзакции.

Формат ссылки для локального варианта КриптоАРМ API

Вариант 1:

```
cryptoarm://<command>/<URI>
```

- `cryptoarm://` - зарегистрированный протокол
- `<command>` - выполняемая команда
- `<URI>` - путь к файлу JSON с параметрами, нужными для выполнения команды

Вариант 2:

```
cryptoarm://<command>/<JSON>
```

- `cryptoarm://` - зарегистрированный протокол
- `<command>` - выполняемая команда
- `<JSON>` - JSON с параметрами, нужными для выполнения команды

Описание запросов и ответов

Все запросы между КриптоАРМ и сервером ДОЛЖНЫ соответствовать спецификации протокола **JSON-RPC 2.0**.

В качестве транспорта используется HTTP. Должен использоваться TLS, незащищенные соединения КриптоАРМ отклоняет.

При включенной настройке «Использовать только набор алгоритмов ГОСТ для подключений по API» КриптоАРМ будет принимать только ГОСТ TLS, остальные шифросюиты будут отклоняться.

POST-запрос

КриптоАРМ выполняет HTTP POST-запросы, которые содержат заголовки:

- `Content-Type`: должен быть application/json.
- `Content-Length`: должен содержать правильную длину в соответствии с HTTP-спецификацией.
- `Accept`: должен быть application/json.

GET-запрос

Не используются.

Ответ

HTTP-ответ сервера должен содержать заголовки:

- `Content-Type`: должен быть application/json.
- `Content-Length`: должен содержать правильную длину в соответствии с HTTP-спецификацией.

Объект Error

В случае ошибки сервер должен отправить ответ следующей структуры:

Ключ	Тип	Описание
code	`number`	Код ошибки
message	`string`	Короткое описание ошибки
data	`string/Object`	Необязательное поле. Может содержать дополнительные сведения об ошибке.

HTTP-коды

Код	Ошибка	Описание
200	OK	И для ответов, и для ошибок
204	No Response	Для пустых запросов (нотификация)
405	Method Not Allowed	Метод не доступен
415	Unsupported Media Type	Если `Content-Type` не application/json

Открыть статью на сайте

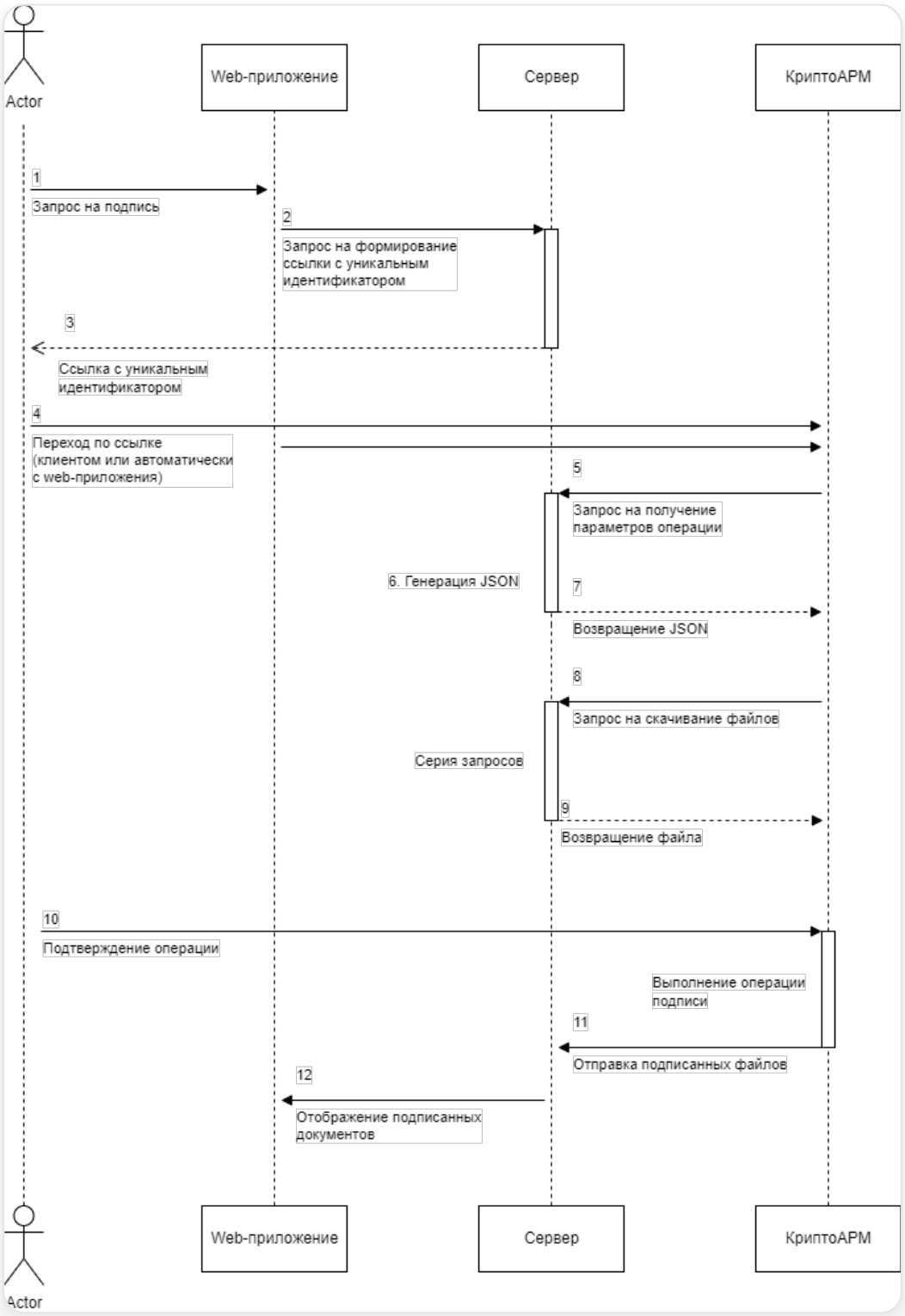
Команда signAndEncrypt

- Общая информация
- Формат ссылки
- Описание запросов и ответов
- Получение параметров операции
- Отправка результата прямых операций
- Отправка результата обратных операций
- Отправка результата проверки подписи
- Интерфейс ISignAndEncryptParameters
- Тип ISignAndEncryptOperationDirect
- Тип ISignAndEncryptOperationReverse
- Тип ISignAndEncryptOperationVerify
- Интерфейс ISignAndEncryptOperationProps
- Интерфейс IFile
- Интерфейс IExtra
- Интерфейс IDirectResults
- Интерфейс IDirectResultOut
- Интерфейс IReverseResults
- Интерфейс IReverseResultOut
- Интерфейс IVerifySignResults
- Интерфейс IVerifySignResult
- Интерфейс ISignerStatus
- Интерфейс ILocalResultParams
- Интерфейс ISignStampAppearance
- Интерфейс IMockupSettings
- Интерфейс IRequisitesSettings
- Интерфейс IPdfCertRequisite
- Интерфейс IPdfMarkedArea
- Интерфейс КриптоАРМ при подписи документов

Общая информация

Команда `signAndEncrypt` (подпись и шифрование) используется для запроса на подпись документа или пакета документов. Может использоваться в качестве аутентификатора.

> 📌 Выполнение операции требует действующей лицензии на КриптоАРМ.



Формат ссылки

Для выполнения команды `signAndEncrypt` должна быть сформирована ссылка вида:

```
cryptoarm://<command>/<URL>/?id=<id>
```

- `cryptoarm://` - зарегистрированный протокол
- `<command>` - выполняемая команда
- `<URL>` - ссылка на получение JSON с параметрами, нужными для выполнения команды
- `?id=<id>` - обязательный параметр. Идентификатор транзакции.

Пример:

```
cryptoarm://signAndEncrypt/https://example.com/json?id=2c48eb32-a0a8-405c-ade9-eed130605cba
```

Описание запросов и ответов

Все запросы между КриптоАРМ и сервером ДОЛЖНЫ соответствовать спецификации протокола JSON-RPC 2.0. В качестве транспорта используется HTTP.

> 🔍 Общее описание указано в разделе Формат ссылки.

Получение параметров операции

После получения команды `signAndEncrypt` КриптоАРМ отправляет запрос на `<URL>` для получения параметров операции.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`signAndEncrypt.parameters`	Используемый метод. Всегда `signAndEncrypt.parameters`.
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию. 🔍 Подробнее в разделе Формат ссылки.
diagnostic	`IDiagnosticInformaton`	Диагностическая информация о рабочем месте

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "signAndEncrypt.parameters",
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
    "diagnostic": {
    }
}
```

Формат ответа

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
result	`ISignAndEncryptParameters`	Объект со сведениями о параметрах операции подписи
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию. 🔍 Подробнее в разделе Формат ссылки
appName?	string	Необязательный параметр. Используется только для локального API. Если значение передано, то КриптоАРМ отобразит это название в окне подтверждения операции как название стороннего приложения.
apiKey?	string	Необязательный параметр. Используется только для локального API. Если значение передано, то КриптоАРМ отобразит это значение в окне подтверждения операции как проверочный код.

Пример:

```
HTTP/1.1 200 OK
Connection: close
Content-Length: ...
Content-Type: application/json
Date: Sat, 08 Jul 2020 12:04:08 GMT
{
```

```
    "jsonrpc": "2.0",
    "result": {
        "operation": [
            "SIGN",
            "ARCHIVE",
            "ENCRYPT"
        ],
        "props": {
            "headerText": "Подпись документов cryptoarm.ru",
            "license": "",
            "files": [{
                    "name": "file1.txt",
                    "url": "http://localhost:8080/public/files/file1.txt",
                    "id": 1,
                    "urlDetached": ""
                },
                {
                    "name": "file2.txt",
                    "url": "http://localhost:8080/public/files/file2.txt",
                    "id": 2,
                    "urlDetached": ""
                },
                {
                    "name": "file4.pdf",
                    "url": "http://localhost:8080/public/files/file4.pdf",
                    "id": 4,
                    "urlDetached": ""
                }
            ],
            "extra": {
                "token": "9c7101f7-9c47-4481-b4da-a6a497abde08",
                "signType": "1",
                "signStandart": "1"
            },
            "uploader": "http://localhost:8080/upload"
        }
    },
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Отправка результата прямых операций

После того, как пользователь выберет нужные сертификаты КриптоАРМ выполняет операцию. Полученные файлы отправляется POST-запросом. Используются нотификации (уведомления), для которых не требуется ответ сервера.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».

Ключ	Значение	Описание
method	`signAndEncrypt.outDirectResults`	Используемый метод. Всегда `signAndEncrypt.outDirectResults`.
params	Объект типа `IDirectResults`	Сведения о результатах прямой операции

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "signAndEncrypt.outDirectResults",
    "params": {
        "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
        "directResults": [
          {
            "id": 2
        "out": "MIIWgQYJKoZIhvcNAQcCoIIWcjCCFm4CA…cN/aHmA="
          }
        ]
    }
}
```

Отправка результата обратных операций

Результаты отправляется POST-запросом. Используются нотификации (уведомления), для которых не требуется ответ сервера.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`signAndEncrypt.outReverseResults`	Используемый метод. Всегда `signAndEncrypt.outReverseResults`.
params	Объект типа `IReverseResults`	Сведения о результатах обратной операции

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "signAndEncrypt.outReverseResults",
    "params": {
        "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
        "reverseResults": [
          {
            "out": "MIIWgQYJKoZIhvcNAQcCoIIWcjCCFm4CA…cN/aHmA="
          }
        ]
    }
}
```

Отправка результата проверки подписи

Результаты проверки подписи отправляется POST запросом. Используются нотификации (уведомления), для которых не требуется ответ сервера.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`signAndEncrypt.verifySignResults`	Используемый метод. Всегда `signAndEncrypt.verifySignResults`.
params	Объект типа `IVerifySignResults`	Сведения о проверке подписи

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "signAndEncrypt.verifySignResults",
    "params": {
        "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
        "verifyResults": [
          {
            "id": 2,
            "status": false,
            "signers": [
              {
```

```
                "hash": "MIIFFDCCBMGgAwIBAgIQTm1HiybyfWV",
                "issuerFriendlyName": "Минкомсвязь России",
                "issuerName": "Минкомсвязь России",
                "subjectFriendlyName ": "Минкомсвязь России",
                "subjectName": "Минкомсвязь России",
                "status": true
              }
            ]
          }
        ]
    }
}
```

Интерфейс ISignAndEncryptParameters

Объекты данного типа описывают вид операции и её параметры.

Свойство	Тип	Описание
operation	string[]	Тип операции. Доступные значения типов (комбинировать различные типы нельзя): `ISignAndEncryptOperationDirect`, `ISignAndEncryptOperationReverse`, `ISignAndEncryptOperationVerify`
props	`ISignAndEncryptOperationProps`	Параметры операции

Тип ISignAndEncryptOperationDirect

Возможные прямые операции.

Значение	Описание
SIGN	Подпись
ARCHIVE	Архивирование
ENCRYPT	Шифрование

Тип ISignAndEncryptOperationReverse

Возможные обратные операции.

Значение	Описание
UNSIGN	Снятие подписи
DECRYPT	Расшифрование
UNZIP	Разархивирование

Тип ISignAndEncryptOperationVerify

Проверка подписи.

Значение	Описание
VERIFYSIGN	Проверка подписи

Интерфейс ISignAndEncryptOperationProps

Интерфейс `ISignAndEncryptOperationProps` описывает параметры операции.

Свойство	Тип	Описание
headerText?	string	Необязательный параметр. Используется для отображения в заголовке окна. Максимальная длина - 40 символов.
descriptionText?	string	Необязательный параметр. Используется для отображения в сведениях об операции. Максимальная длина - 120 символов.
license?	string	Необязательное свойство. Содержит временную лицензию, которая будет использоваться для выполнения операции в КриптоАРМ.
uploader	string	Ссылка, на которую будут отправлены или сохранены результаты операции. Поддерживает протоколы https:// и file://
files	Массив типа `IFile[]`	

Свойство	Тип	Описание
		Массив файлов на подпись. Если не передан, то должен быть передан параметр `archive`
archive	`IFile[]`	Архив файлов на подпись. Распаковываются после получения. Параметр может использоваться вместо `files`. Перед отправкой результатов операции на сервер, они будут упакованы в архив.
extra	Объект типа `IExtra`	Настройки операции
localResultParams	Объект типа `ILocalResultParams`	Необязательное свойство. Используется только для локального API. Указывает пути для сохранения результатов.

Интерфейс IFile

Интерфейс `IFile` описывает файлы и ссылки на них.

Свойство	Тип	Описание
name	string	Имя файла (с расширением)
url	string	Ссылка на скачивание файла
id	string	Уникальный идентификатор файла
urlDetached?	string	Необязательный параметр. Используется для откреплённой подписи.

Интерфейс IExtra

Интерфейс `IExtra` описывает настройки операции.

Если параметр не задан, то пользователю доступен выбор из всех доступных в приложении значений.

Свойство	Тип	Описание
signType?	number	

Свойство	Тип	Описание
		Необязательный параметр. Возможные значения: - 0 - присоединенная подпись, - 1 - отсоединённая подпись.
signStandart?	number	Необязательный параметр. Стандарт подписи. Возможные значения: - 0 - CMS, - 1 - CAdES-X Long Type 1, - 2 - CAdES-T, - 3 - CAdES-A.
signEncoding?	number	Необязательный параметр. Кодировка. Возможные значения: - 0 – BASE-64, - 1 – DER.
timestampOnSign?	string	Необязательный параметр. Штамп времени на подпись. Возможные значения: - True - будет добавлен штамп времени, - False – не будет добавлен штамп времени.
timestampOnData?	string	Необязательный параметр. Штамп времени на подписываема данные. Возможные значения: - True - будет добавлен штамп времени, - False – не будет добавлен штамп времени.
encryptEncoding?	number	Необязательный параметр. Кодировка. Возможные значения: - 0 – BASE-64, - 1 – DER.
encryptAlgorithm?	number	Необязательный параметр. Алгоритм шифрования. Возможные значения: - 0 – ГОСТ 28147-89, - 1 – ГОСТ 34.12-2015 Магма, - 2 – ГОСТ 34.12-2015 Кузнечик.
token?	string	

Свойство	Тип	Описание
		Необязательный параметр. Токен, который будет использоваться при скачивании файлов с сервиса (параметр запроса).
tspURL?	string	Необязательный параметр. Адрес службы штампов времени.
ocspURL?	string	Необязательный параметр. Адрес службы актуальных статусов.
encryptCertificates?	string[]	Необязательный параметр. Сертификаты шифрования.
signCertificate?	Объект типа: `{«x509»:string}`	Необязательный параметр. Сертификат подписчика или параметры для поиска сертификата подписчика.
signatureExtension?	string	Необязательный параметр. Расширение для подписанного файла.
separateArchivesForSignResults?	boolean	Необязательный параметр. Создавать пакет (архив) для каждого подписываемого файла.
isAddStampToPdf?	boolean	Необязательный параметр. Добавить печатную форму для PDF-файлов.
signStampAppearance?	`ISignStampAppearance`	Необязательный параметр. Параметры штампа PDF.
signStampPosition?	`IPdfMarkedArea`	Необязательный параметр. Расположение и размер области под штамп.

Интерфейс IDirectResults

Объекты данного типа описывают результаты прямой операции.

Свойство	Тип	Описание
id	string	

Свойство	Тип	Описание
		Используется идентификатор, который указан в ссылке на операцию. 🔍 Формат ссылки
status	string	Статус выполнения операции. В случае успеха «Completed».
directResults	`IDirectResultOut[]`	Массив результатов прямых операций

Интерфейс IDirectResultOut

Объекты данного типа содержат результаты прямой операции для файла.

Свойство	Тип	Описание
id	string	Необязательный параметр. Идентификатор исходного файла. Если включено архивирование, то данный параметр не используется, т.к. выходной файл один для всех исходных.
out	string	Результат операции в `BASE-64`
signers?	`ISignerStatus[]`	Необязательный параметр. Сведения о подписчиках.
signValid?	boolean	Необязательный параметр. Общий статус подписи. Учитывается статус всех подписей файла.

Интерфейс IReverseResults

Объекты данного типа описывают результаты обратной операции.

Свойство	Тип	Описание
id	string	Используется идентификатор, который указан в ссылке на операцию. 🔍 Формат ссылки
reverseResults	`IReverseResultOut[]`	

Свойство	Тип	Описание
		Массив результатов обратных операций

Интерфейс IReverseResultOut

Объекты данного типа описывают результаты обратной операции.

Свойство	Тип	Описание
id	string	Необязательный параметр. Идентификатор исходного файла.
out	string	Результат операции в BASE-64

Интерфейс IVerifySignResults

Объекты данного типа описывают результаты проверки подписи.

Свойство	Тип	Описание
id	string	Используется идентификатор, который указан в ссылке на операцию. 🔍 Формат ссылки
status	string	Статус выполнения операции. В случае успеха « Completed».
verifySignResults	`IVerifySignResult[]`	Массив результатов проверки

Интерфейс IVerifySignResult

Объекты данного типа описывают результаты проверки подписи.

Свойство	Тип	Описание
id	string	Идентификатор исходного файла
signValid	boolean	Общий статус проверки подписи
signers	`ISignerStatus[]`	Информация о подписчиках документа

Интерфейс ISignerStatus

Объекты данного типа описывают сведения о подписчиках.

Свойство	Тип	Описание
signerCertificate	`ICertificateInfo`	Сведения о сертификате подписчика
isValid	boolean	Статус подписи
signingTime	string	Время подписи

Интерфейс ILocalResultParams

Объекты данного типа используется только в параметрах локального API.

Содержат пути для сохранения результатов операций.

Свойство	Тип	Описание
savePath?	string	Необязательный параметр. Путь для сохранения результатов операции.
saveResultsSeparately?	boolean	Необязательный параметр. Определяет, сохранять ли результаты по каждому файлу в отдельный файл или сохранять в один JSON, один файл.

Интерфейс ISignStampAppearance

Интерфейс `ISignStampAppearance` описывает параметры для штампа PDF.

Свойство	Тип	Описание
mockupSettings	`IMockupSettings`	Настройки внешнего вида штампа подписи
requisitesSettings	`IRequisitesSettings`	Настройки содержимого штампа (реквизиты)
pageSelection	string	

Свойство	Тип	Описание
		Определяет, на какой странице или страницах будет отображаться штамп. Возможные значения: - «all» – штамп на всех страницах, - «last» – штамп на последней странице, - «some» – штамп на некоторых страницах.
pageNumbers?	string	Необязательный параметр. Страница или диапазон страниц. Пример: «3» или «1-7».

Интерфейс IMockupSettings

Интерфейс `IMockupSettings` описывает параметры внешнего вида штампа.

Свойство	Тип	Описание
position	string	Положение штампа внутри области. Возможные значения: - «fitArea» – вписать, - «actualSize» – реальный размер, - «fitMockup» – подогнать область под макет.
addBackground	boolean	Определяет, будет ли добавлен фон на область
addBorders	boolean	Определяет, будет ли добавлена граница на область
logotype?	boolean	Необязательный параметр. Использовать или нет логотип для штампа.

Интерфейс IRequisitesSettings

Интерфейс `IRequisitesSettings` описывает содержимое (реквизиты) штампа подписи.

Свойство	Тип	Описание
position	string	Реквизиты в штампе. Возможные значения: - «default» – штамп без дополнительных областей под реквизиты, - «left» – штамп с дополнительными реквизитами слева, - «right» – штамп с дополнительными реквизитами справа, - «leftAndRight» – штамп с дополнительными реквизитами слева и справа.
centralDisplayType	string	Внешний вид штампа. Определяет доступность настроек дополнительных реквизитов. Возможные значения: - «byGost» – внешний вид по ГОСТ, - «arbitrary» – произвольно.
central	`IPdfCertRequisite[]`	Массив значений реквизитов, для добавления в центральную часть штампа
left	`IPdfCertRequisite[]`	Массив значений реквизитов, для добавления в левую часть штампа
right	`IPdfCertRequisite[]`	Массив значений реквизитов, для добавления в правую часть штампа

Интерфейс IPdfCertRequisite

Интерфейс `IPdfCertRequisite` описывает свойства для реквизита штампа.

Свойство	Тип	Описание
title	string	Заголовок
dataKey?	string	Необязательный параметр. Указывает название поля сертификата, значение которого

Свойство	Тип	Описание
		будет использовано. Если в сертификате нет указанного поля, то значение будет «Не указано».
isEditable	boolean	Указывает, доступно ли редактирование поля пользователем. Если `false`, то значение должно быть передано в поле `editedValue` или взято из сертификата по значению `dataKey`.
editedValue?	string	Необязательный параметр. Значение реквизита, которое будет использовано, если не указано свойство `dataKey`.
editedValueCharLimit?	number	Необязательный параметр. Определяет максимальную длину строки.

Интерфейс IPdfMarkedArea

Интерфейс `IPdfMarkedArea` описывает параметры для расположения области штампа PDF (координаты и размеры).

Свойство	Тип	Описание
height	number	Высота области под штамп
width	number	Ширина области под штамп
horizontalPadding	number	Отступ от левого края документа
verticalPadding	number	Отступ от правого края документа

Интерфейс КриптоАРМ при подписи документов

При выполнении операции подписи по ссылке, не относящийся к процедуре интерфейс блокируется.

Пользователю доступны: выбор сертификата, часть настроек подписи.

Кнопка «Выполнить» заменяется двумя: «Подпись» и «Отмена». После выполнения команды, приложение будет свернуто в системный трей.

Открыть статью на сайте

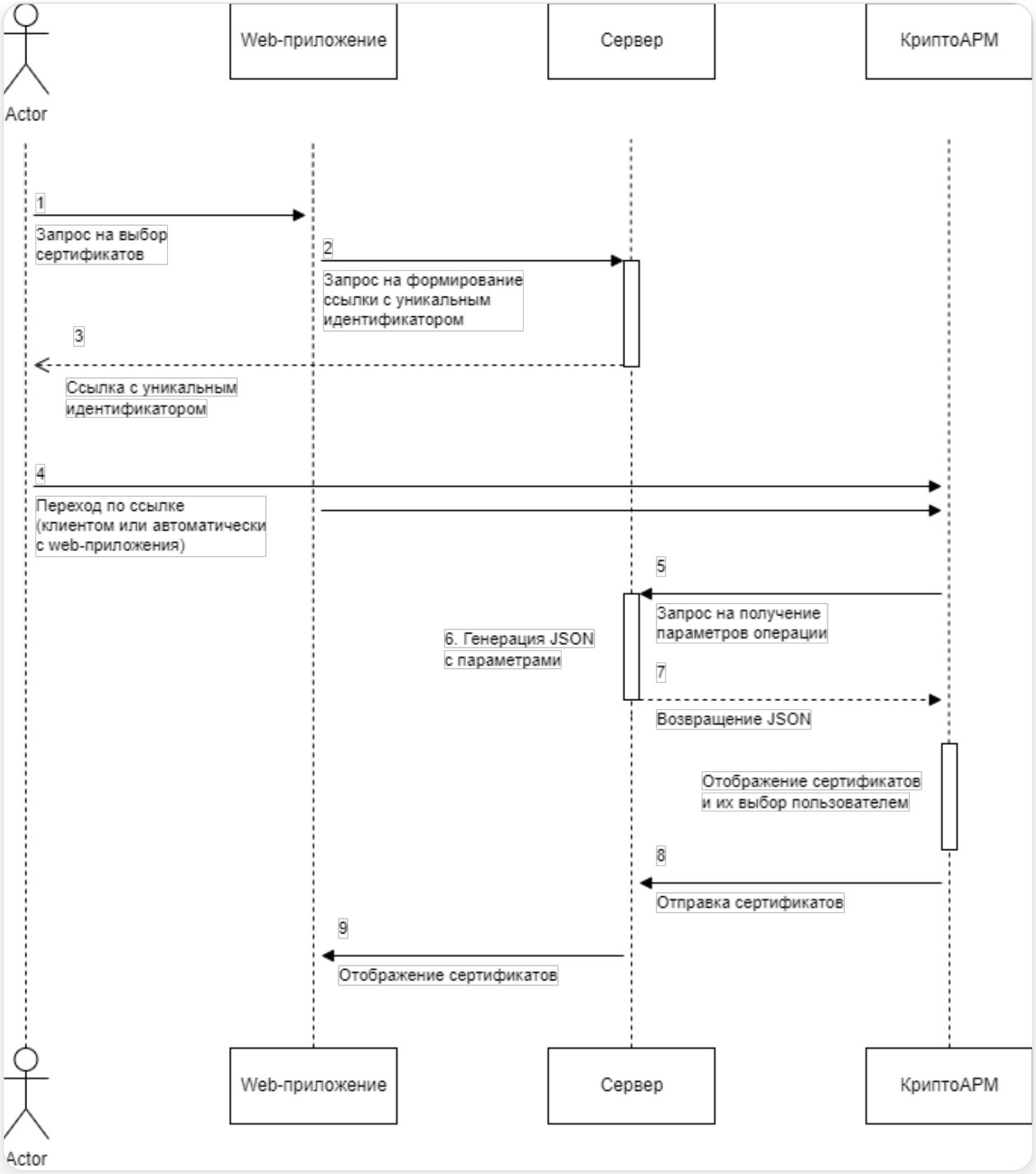
Команда certificates

- Общая информация
- Формат ссылки
- Получение параметров операции
- Отправка сертификата
- Отправка списка сертификатов
- Отправка сведений о сертификате
- Интерфейс ICertificatesParameters
- Интерфейс ICertificatesOperationProps
- Интерфейс ICertificateBase64Params
- Интерфейс ICertificateInfo
- Интерфейс ICertificateIdentityInfo
- Интерфейс КриптоАРМ при выборе и отправке сертификатов

Общая информация

Команда `certificates` используется для: экспорта сертификата или списка сертификатов, а импорта сертификата в локальное хранилище, просмотра информации о сертификате.

Схема взаимодействия (экспорт сертификатов):



Все запросы между КриптоАРМ и сервером ДОЛЖНЫ соответствовать спецификации протокола JSON-RPC 2.0.

В качестве транспорта используется HTTP.

> 🔍 Общее описание указано в разделе Формат ссылки.

Формат ссылки

Для выполнения команды `certificates` должна быть сформирована ссылка вида:

```
cryptoarm://certificates/<URL>/?id=<id>
```

- `cryptoarm://` - зарегистрированный протокол
- `certificates` - выполняемая команда
- `<URL>` - ссылка, на которую КриптоАРМ будет слать запросы
- `id` - уникальный идентификатор транзакции

Пример:

```
cryptoarm://certificates/https://example.com/json?id=2c48eb32-a0a8-405c-ade9-eed130605cba
```

Получение параметров операции

После получения команды `certificates` КриптоАРМ отправляет запрос на получение параметров операции.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`certificates.parameters`	Используемый метод. Всегда `certificates.parameters`.
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию. 🔍 Формат ссылки
diagnostic	`IDiagnosticInformaton`	Диагностическая информация о рабочем месте

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "certificates.parameters",
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
```

```
    "diagnostic": {
     }
}
```

Формат ответа

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
result	`ICertificatesParameters`	Объект со сведениями о параметрах операции
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию. 🔍 Формат ссылки

Пример ответа для экспорта сертификата:

```
HTTP/1.1 200 OK
Connection: close
Content-Length: ...
Content-Type: application/json
Date: Sat, 08 Jul 2020 12:04:08 GMT
{
    "jsonrpc": "2.0",
    "result": {
        "operation": "export",
        "props": {
            "store": ["MY"],
            "multy": false
        }
    },
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Пример ответа для экспорта сертификата:

```
HTTP/1.1 200 OK
Connection: close
Content-Length: ...
Content-Type: application/json
Date: Sat, 08 Jul 2020 12:04:08 GMT
{
    "jsonrpc": "2.0",
    "result": {
        "operation": "information",
        "props": {
```

```
            "certificateBase64": "MIIFFDCCBMGgAwIBAgIQT...4VVkDWbX/n4="
        }
    },
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Отправка сертификата

При экспорте сертификатов результат отправляются на сервер. После того, как пользователь выберет нужный сертификат КриптоАРМ отправляет запрос, содержащий выбранные элементы (base64 без заголовков). Используются нотификации (уведомления), для которых не требуется ответ сервера.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`certificates.base64`	Используемый метод. Всегда `certificates.base64`.
params	`ICertificateBase64Params`	Параметры, содержащие объект сертификата

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "certificates.base64",
    "params": {
        "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
        "certificateBase64": "MIIFFDCCBMGgAwIBAgIQTm1HiybyfWV...4VVkDWbX/n4=",
        "friendlyName": "Минкомсвязь России"
    }
}
```

Отправка списка сертификатов

При экспорте сертификатов результат отправляются на сервер. Если параметры `ICertRequestParameters` содержат поле «multy» со значением «true», то пользователю в КриптоАРМ будет разрешён множественный выбор сертификатов. После того, как пользователь выберет нужные сертификаты и нажмет кнопку «Готово», КриптоАРМ отправляет запрос, содержащий выбранные элементы (`base64` без заголовков). Используются нотификации (уведомления), для которых не используется ответ сервера.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`certificates.base64`	Используемый метод. Всегда `certificates.base64`.
params	`ICertificateBase64Params`	Параметры, содержащие объект сертификата

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "certificates.base64",
    "params": {
        "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
        "certificates": [{
                "certificateBase64": "MIIFFDCCBMGgAwIBAgIQTm1HiybyfWV...4VVkDWbX/
n4=",
                "friendlyName": "Минкомсвязь России"
            },
            {
                "certificateBase64": "MIIFFDCCBMGgAwIBAgIQTm1HiybyfWV...4VVkDWbX/
n4=",
                "friendlyName": "Головной удостоверяющий центр"
            }
        ]
    }
}
```

Отправка сведений о сертификате

После того, как пользователь выберет нужный сертификат КриптАРМ отправляет запрос, содержащий выбранные элементы (base64 без заголовков). Используются нотификации (уведомления), для которых не требуется ответ сервера.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`certificates.information`	Используемый метод. Всегда `certificates.information`.
params	Объект типа `ICertificateInfo`	Сведения о сертификате

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "certificates.information",
    "params": {
        "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
        "hash": "MIIFFDCCBMGgAwIBAgIQTm1HiybyfWV",
        "issuerFriendlyName": "Минкомсвязь России",
        "issuerName": "Минкомсвязь России",
        "subjectFriendlyName ": "Минкомсвязь России",
        "subjectName": "Минкомсвязь России",
        "status": true
    }
}
```

Интерфейс ICertificatesParameters

Объекты данного типа описывают параметры команды запроса на получение сертификат.

Свойство	Тип	Описание
operation	string	Тип операции импорт, экспорт, информация. Доступные значения: “import”, “export”, “information”
props	`ICertificatesOperationProps`	Параметры операции

Интерфейс ICertificatesOperationProps

Объекты данного типа описывают дополнительные свойства операции.

Свойство	Тип	Описание
headerText?	string	Необязательный параметр. Используется для отображения в заголовке окна. Максимальная длина - 40 символов.
descriptionText?	string	Необязательный параметр. Используется для отображения в сведениях об операции. Максимальная длина - 120 символов.
store?	string[]	Необязательный параметр. Массив имен хранилищ. Если не задан, то используется значение `MY` (личные сертификаты).
multy?	boolean	Необязательный параметр. Разрешен ли множественный выбор. По умолчанию `false`.
certificateBase64?	string	Необязательный параметр. Сертификат в формате `X.509` закодированный в `Base64`.

Интерфейс ICertificateBase64Params

Объекты данного типа описывают параметры запроса для метода `certificates.base64`.

Свойство	Тип	Описание
id	string	Идентификатор транзакции
certificateBase64	string	Сертификат в формате `X.509` закодированный в `Base64`
friendlyName	string	Дружественное имя сертификата

Интерфейс ICertificateInfo

Объекты данного типа описывают объекты, содержащие свойства сертификата.

Свойство	Тип	Описание
hash	string	SHA1 отпечаток
issuerFriendlyName	string	Дружественное имя издателя (CN)
issuerName	string	Имя издателя
notAfter	string	Дата окончания действия сертификата
notBefore	string	Дата начала действия сертификата
rootCAMinComSvyaz	boolean	Флаг, обозначающий является ли владельцем корневого сертификата цепочки “Минкомсвязь России”
subjectFriendlyName	string	Дружественное имя субъекта (CN)
subjectName	string	Имя субъекта
status	boolean	Статус сертификата. Проверяется вся цепочка.
serial	string	Серийный номер сертификата
x509?	string	Необязательный параметр. Сертификат в формате `X.509` закодированный в `Base64`.

Интерфейс ICertificateIdentityInfo

Объекты данного типа описывают объекты, содержащие параметры сертификата, позволяющие только идентифицировать его.

Свойство	Тип	Описание
hash	string	SHA1-отпечаток сертификата
notAfter	string	Дата окончания действия сертификата

Свойство	Тип	Описание
notBefore	string	Дата начала действия сертификата
isSelfSigned	boolean	Флаг самоподписанного сертификата
key	boolean	Наличие привязки к закрытому ключу
pubKeyAlg	string	Алгоритм публичного ключа
issuerFriendlyName	string	Дружественное имя издателя (CN)
issuerName	string	Имя издателя
subjectFriendlyName	string	Дружественное имя субъекта (CN)
subjectName	string	Имя субъекта
signatureAlgorithm	string	Алгоритм подписи
signatureDigestAlgorithm	string	Алгоритм хеширования
serial	string	Серийный номер сертификата
organizationName	string	Название организации
provider	string	Тип криптопровайдера
keyUsageString	string	Использование ключа
keyNotAfter	number	Срок действия закрытого ключа (timestamp)

Интерфейс КриптоАРМ при выборе и отправке сертификатов

При выполнении команды запроса на сертификаты, не относящийся к процедуре интерфейс блокируется.

Пользователю доступны:

- Выбор сертификатов,
- Две кнопки: «Готово» и «Отмена».

После выполнения команды, приложение будет свернуто в системный трей.

Открыть статью на сайте

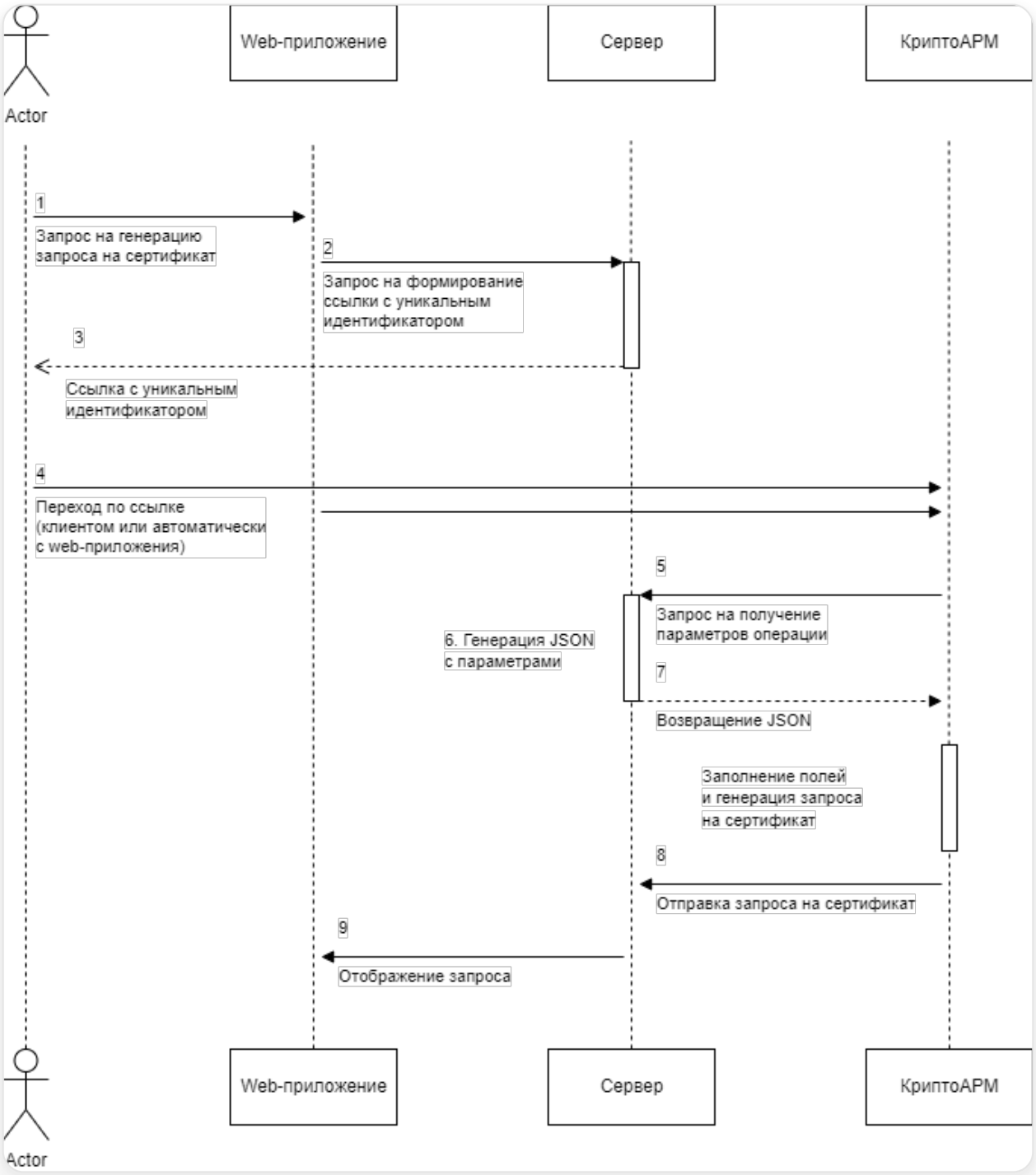
Команда `certrequests`

- Общая информация
- Формат ссылки
- Получение параметров операции
- Отправка запроса на сертификат
- Интерфейс ICertrequestsParameters
- Тип CertrequestsOperation
- Интерфейс ICertrequestsOperationGenerateProps
- Интерфейс ICertificatesParameters
- Интерфейс IJSONTemplate
- Интерфейс IRDN
- Интерфейс IRequestExtension
- Интерфейс IKeyUsage
- Интерфейс IExtendedKeyUsage
- Интерфейс ICertificateTemplate
- Интерфейс ICertificaterequestBase64Params
- Интерфейс КриптоАРМ при выборе и отправке сертификатов

Общая информация

Команда `certrequests` используется для: генерации запроса на сертификат по шаблону или экспорт запросов.

Схема взаимодействия (экспорт сертификатов):



Все запросы между КриптоАРМ и сервером ДОЛЖНЫ соответствовать спецификации протокола JSON-RPC 2.0.

В качестве транспорта используется HTTP.

> 🔍 Общее описание указано в разделе Формат ссылки.

Формат ссылки

Для выполнения команды `certrequests` должна быть сформирована ссылка вида:

```
cryptoarm://certificates/<URL>/?id=<id>
```

- `cryptoarm://` - зарегистрированный протокол
- `certrequests` - выполняемая команда
- `<URL>` - ссылка, на которую КриптоАРМ будет слать запросы
- `id` - уникальный идентификатор транзакции

Пример:

```
cryptoarm://certrequests/https://example.com/json?id=2c48eb32-a0a8-405c-ade9-eed130605cba
```

Получение параметров операции

После получения команды `certrequests` КриптоАРМ отправляет запрос на получение параметров операции.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`certrequests.parameters`	Используемый метод. Всегда `certrequests.parameters`.
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию. 🔍 Формат ссылки
diagnostic	`IDiagnosticInformaton`	Диагностическая информация о рабочем месте

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "certrequests.parameters",
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
```

```
    "diagnostic": {
    }
}
```

Формат ответа

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
result	`ICertrequestsParameters`	Объект со сведениями о параметрах операции
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию. 🔍 Формат ссылки

Пример ответа:

```
HTTP/1.1 200 OK
Connection: close
Content-Length: ...
Content-Type: application/json
Date: Sat, 08 Jul 2020 12:04:08 GMT
{
    "jsonrpc": "2.0",
    "result": {
        "operation": "GENERATE",
        "props": {
            "templateType": "JSONTemplate",
            "template": {
                "Description": "",
                "FriendlyName": "Пользователь",
                "RDN": [{
                    "Oid": "2.5.4.3",
                    "Name": "CN",
                    "Length": 64,
                    "LocalizedName": "Общее имя",
                    "SettingsValues": [],
                    "DefaultValue": null,
                    "ProhibitAnyValue": false,
                    "ProhibitChange": false,
                    "ProhibitEmpty": true
                }],
                "Extensions": {
                    "KeyUsage": [{
                        "Name": "cRLSign",
                        "LocalizedName": "Автономное подписание списка отзыва
(CRL)",
                        "DefaultValue": false,
                        "ProhibitChange": true
                    }],
```

```
                    "ExtendedKeyUsage": [{
                        "Name": "1.3.6.1.5.5.7.3.1",
                        "LocalizedName": "Проверка подлинности сервера",
                        "DefaultValue": false,
                        "ProhibitChange": true
                    }]
                },
                "MarkExportable": false
            },
            "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
        }
    }
}
```

Отправка запроса на сертификат

После генерации запроса, он будет отправлен на сервер. Используются нотификации (уведомления), для которых не требуется ответ сервера.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`certrequests.base64`	Используемый метод. Всегда `certrequests.base64`.
params	`ICertificaterequestBase64Param`	Параметры, содержащие объект сертификата

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "certrequests.base64",
    "params": {
        "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
        "certificaterequestBase64": "MIIFFDCCBMGgAwIBAgIQTm1HiybyfWV...4VVkDWbX/
n4=",
        "friendlyName": "ООО Рога и Копыта"
    }
}
```

Интерфейс ICertrequestsParameters

Объекты данного типа описывают параметры команды.

Свойство	Тип	Описание
operation	string	Тип операции: генерация запроса на сертификат. Значение типа: `CertrequestsOperation
props	`ICertrequestsOperationGenerateProps`	Параметры операции

Тип CertrequestsOperation

Возможные операции с запросами на сертификат.

Значение	Описание
GENERATE	Генерация запроса на сертификат

Интерфейс ICertrequestsOperationGenerateProps

Объекты данного типа описывают дополнительные свойства операции.

Свойство	Тип	Значение	Описание
headerText?	string	Необязательный параметр. Используется для отображения в заголовке окна. Максимальная длина: 40 символов.	`headerText?`
descriptionText?	string	Необязательный параметр. Используется для отображения в сведениях об операции. Максимальная длина: 120 символов.	`descriptionText?`
templateType	string	`JSONTemplate` или `CertificateTemplate`	В качестве шаблона используется JSON типа `IJSONTemplate` или в

Свойство	Тип	Значение	Описание
			качестве шаблона используется сертификат
template	`IJSONTemplate` или `ICertificateTemplate`	Шаблон для генерации запроса на сертификат	

Интерфейс ICertificatesParameters

Объекты данного типа описывают поля для генерации запроса на сертификат.

Свойство	Тип	Описание
Description	string	Описание шаблона
FriendlyName	string	Дружественное имя шаблона
RDN	`IRDN[]`	Набор полей DN
Extensions	`IRequestExtension`	Расширения
MarkExportable	boolean	Определяет экспортируемость ключей

Интерфейс IJSONTemplate

Свойство	Тип	Описание
Description	string	Описание шаблона
FriendlyName	string	Дружественное имя шаблона
RDN	IRDN[]	Набор полей DN
Extensions	IRequestExtension	Расширения
MarkExportable	boolean	Определяет экспортируемость ключей

Интерфейс IRDN

Свойство	Тип	Описание
Oid	string	Описание шаблона
Name	string	Наименование OID
Length	number	Максимальная длина поля
LocalizedName	string	Локализованное наименование OID
SettingsValues	string[]	Список возможных значений
DefaultValue	string	Значение по умолчанию
ProhibitAnyValue	boolean	Флаг указывающий, что пользователю доступны только значения из массива `SettingsValues`
ProhibitChange	boolean	Флаг указывающий, что поле не может быть изменено
ProhibitEmpty	boolean	Флаг указывающий, что поле должно быть непустым

Интерфейс IRequestExtension

Свойство	Тип	Описание
KeyUsage	`IKeyUsage[]`	Описание шаблона
ExtendedKeyUsage	`IExtendedKeyUsage[]`	Наименование OID

Интерфейс IKeyUsage

Свойство	Тип	Описание
Name	string	Наименование OID
LocalizedName	string	Локализованное наименование OID
DefaultValue	boolean	Значение по умолчанию

Свойство	Тип	Описание
ProhibitChange	boolean	Флаг указывающий, что поле не может быть изменено

Интерфейс IExtendedKeyUsage

Свойство	Тип	Описание
Name	string	Наименование OID
LocalizedName	string	Локализованное наименование OID
DefaultValue	boolean	Значение по умолчанию
ProhibitChange	boolean	Флаг указывающий, что поле не может быть изменено

Интерфейс ICertificateTemplate

Объекты данного типа используются для генерации запроса на сертификат, где запрос формируется по сертификату.

Свойство	Тип	Описание
certificateBase64	string	Сертификат в формате `X.509` закодированный в `Base64`

Интерфейс ICertificaterequestBase64Params

Свойство	Тип	Описание
id	string	Идентификатор транзакции
certificaterequestBase64	string	Запрос в формате `X.509` закодированный в `Base64`
friendlyName	string	Дружественное имя субъекта

Интерфейс КриптоАРМ при выборе и отправке сертификатов

При выполнении команды запроса на сертификаты, не относящийся к процедуре интерфейс блокируется.

Пользователю доступны:

- Выбор сертификатов,
- Кнопки «Готово» и «Отмена».

После выполнения команды, приложение будет свернуто в системный трей.

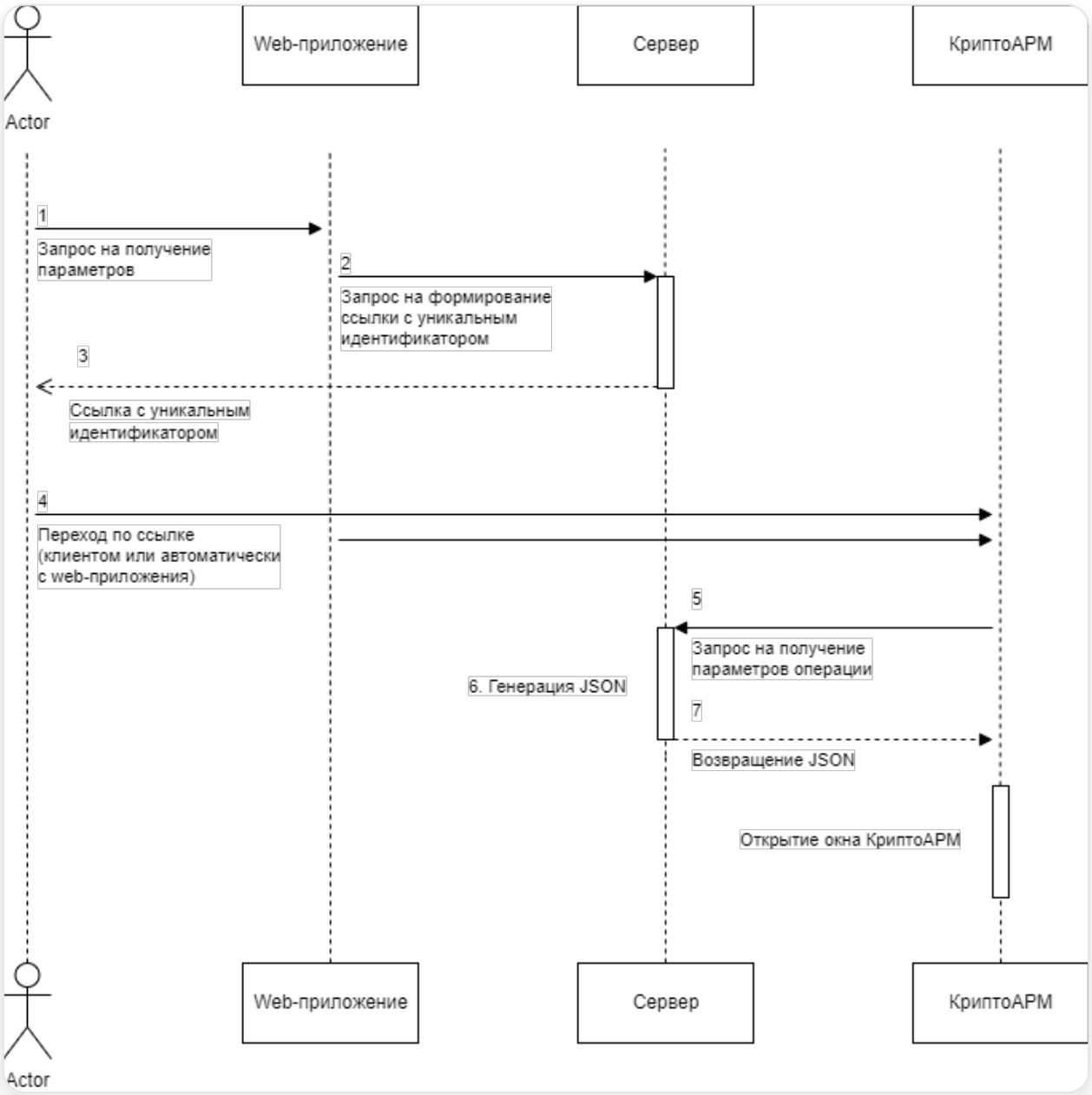
Открыть статью на сайте

Команда diagnostics

- Общая информация
- Формат ссылки
- Получение параметров операции
- Отправка сведений о рабочем месте
- Интерфейс IDiagnosticsParameters
- Тип IDiagnosticOperation
- Интерфейс IDiagnosticsOperationProps
- Интерфейс IDiagnosticsInformation
- Интерфейс ISystemInformation
- Интерфейс IVersions
- Интерфейс IProviders
- Интерфейс ILicenses
- Интерфейс ILicenseInfo
- LicenseType Enum

Общая информация

Команда `diagnostics` используется для диагностики рабочего места пользователя. Схема взаимодействия:ката или списка сертификатов, а импорта сертификата в локальное хранилище, просмотра информации о сертификате.



Все запросы между КриптоАРМ и сервером ДОЛЖНЫ соответствовать спецификации протокола JSON-RPC 2.0.

В качестве транспорта используется HTTP.

> 🔍 Общее описание указано в разделе Формат ссылки.

Формат ссылки

Для выполнения команды `diagnostics` должна быть сформирована ссылка вида:

```
cryptoarm://diagnostics/<URL>/?id=<id>
```

- `cryptoarm://` - зарегистрированный протокол
- `diagnostics` - выполняемая команда
- `<URL>` - ссылка, на которую КриптоАРМ будет слать запросы
- `id` - уникальный идентификатор транзакции

Пример:

```
cryptoarm://diagnostics/https://example.com/json?id=2c48eb32-a0a8-405c-ade9-eed130605cba
```

Получение параметров операции

После получения команды `diagnostics` КриптоАРМ отправляет запрос на получение параметров операции.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`diagnostics.parameters`	Используемый метод. Всегда `diagnostics.parameters`.
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию. 🔍 Формат ссылки
diagnostic	`IDiagnosticInformaton`	Диагностическая информация о рабочем месте

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "certificates.parameters",
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
    "diagnostic": {
     }
}
```

Формат ответа

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
result	`IDiagnosticsParameters`	Объект со сведениями о параметрах операции
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию. 🔍 Формат ссылки

Пример ответа:

```
HTTP/1.1 200 OK
Connection: close
Content-Length: ...
Content-Type: application/json
Date: Sat, 08 Jul 2020 12:04:08 GMT
{
    "jsonrpc": "2.0",
    "result": {
        "operation": ["CSP_ENABLED", "LICENSES", "VERSIONS"],
        "props": {
            "headerText": "Диагностика cryptoarm.ru",
            "descriptionText":
"Выполняется диагностика рабочего места для работы на портале"
        }
    },
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Отправка сведений о рабочем месте

Полученные сведения отправляется POST запросом. Используются нотификации (уведомления), для которых не требуется ответ сервера.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`diagnostics.information`	

Ключ	Значение	Описание
		Используемый метод. Всегда `diagnostics.information`.
params	`IDiagnosticsInformation`	Сведения о рабочем месте

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
  "jsonrpc": "2.0",
  "method": "diagnostics.information",
  "params": {
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
    "CSP_ENABLED": true,
    "LICENSES": {
      "csp": {
        "status": true,
      },
      "cryptoarm": {
        "status": true,
        "type": "temporary",
        "expiration": "1591689487056",
      }
    },
    "VERSIONS": {
      "csp": "5.0.11753",
      "cryptoarm": "2.5.2",
    }
  }
}
```

Интерфейс IDiagnosticsParameters

Объекты данного типа описывают вид операции и её параметры.

Свойство	Тип	Описание
operation	string	Тип операции. Доступные значения типа: `IDiagnosticOperation
props	`IDiagnosticsOperationProps`	Параметры операции

Тип IDiagnosticOperation

Возможные операции.

Значение	Описание
SYSTEMINFORMATION	Сведения о системе
CSP_ENABLED	Наличие КриптоПро CSP
CADES_ENABLED	Доступность CADES
VERSIONS	Версии используемых компонентов (КриптоАРМ, КриптоПро)
PROVIDERS	Список криптопровайдеров
LICENSES	Статус лицензий
PERSONALCERTIFICATES	Наличие личных сертификатов

Интерфейс IDiagnosticsOperationProps

Интерфейс `IDiagnosticsOperationProps` описывает параметры операции.

Свойство	Тип	Описание
headerText?	string	Необязательный параметр. Используется для отображения в заголовке окна. Максимальная длина - 40 символов.
descriptionText?	string	Необязательный параметр. Используется для отображения в сведениях об операции. Максимальная длина - 120 символов.

Интерфейс IDiagnosticsInformation

Объекты данного типа описывают объекты, содержащие сведения о рабочем месте.

Свойство	Тип	Описание
id	string	Идентификатор транзакции
API_VERSION	string	

Свойство	Тип	Описание
		Версия поддерживаемого КриптоАРМ API
SYSTEMINFORMATION	`ISystemInformation`	Сведения о системе
CSP_ENABLED	boolean	Установлен или нет КриптоПро CSP
CADES_ENABLED	boolean	Доступность CADES
VERSIONS	`IVersions`	Версии компонентов
PROVIDERS	`IProviders`	Сведения о провайдерах
LICENSES	`ILicenses`	Сведения о лицензиях

Интерфейс ISystemInformation

Объекты данного типа содержат сведения о системе пользователя.

Свойство	Тип	Описание
type	string	Тип системы. Возможные значения: `Linux`, `Darwin` и `Windows_NT`
arch	string	Архитектура операционной системы. Возможные значения: `arm`, `arm64`, `ia32`, `mips`, `mipsel`, `ppc`, `ppc64`, `s390`, `s390x`, `x32`, и `x64`
platform	string	Имя платформы. Возможные значения: `aix`, `darwin`, `freebsd`, `linux`, `openbsd`, `sunos`, и `win32`
packageType?	string	Необязательный параметр. Тип поддерживаемого пакета (инсталлятора). Возможные значения: `msi`, `pkg`, `rpm` или `deb`

Интерфейс IVersions

Объекты данного типа содержат сведения о версиях.

Свойство	Тип	Описание
csp	string	Версия КриптоПро CSP
cryptoarm	string	Версия КриптоАРМ
openssl	string	Версия OpenSSL

Интерфейс IProviders

Объекты данного типа описывают доступность ГОСТ-провайдеров.

Свойство	Тип	Описание
GOST2012_256	boolean	ГОСТ 2012-256
GOST2012_512	boolean	ГОСТ 2012-512
openssl	boolean	Открытая криптография

Интерфейс ILicenses

Объекты данного типа описывают статусы лицензии КриптоАРМ и КритпоПро CSP.

Свойство	Тип	Описание
csp	`ILicenseInfo`	Сведения о лицензии на КриптоПро CSP
cryptoarm	`ILicenseInfo`	Сведения о лицензии на КриптоАРМ

Интерфейс ILicenseInfo

Объекты данного типа описывают сведения о лицензии компонента.

Свойство	Тип	Описание
status	boolean	Действительна или нет лицензия
type	`LicenseType`	Тип лицензии
expiration?	string	

Свойство	Тип	Описание
		Необязательный параметр. Дата истечения лицензии для трилальных лицензий или подписок (в формате UTC).

LicenseType Enum

Данное перечисление описывает возможные типы лицензий.

Значение	Описание
Permanent	Постоянная
Subscription	Подписка
Daily	Дневная
Trial	Триальная

Открыть статью на сайте

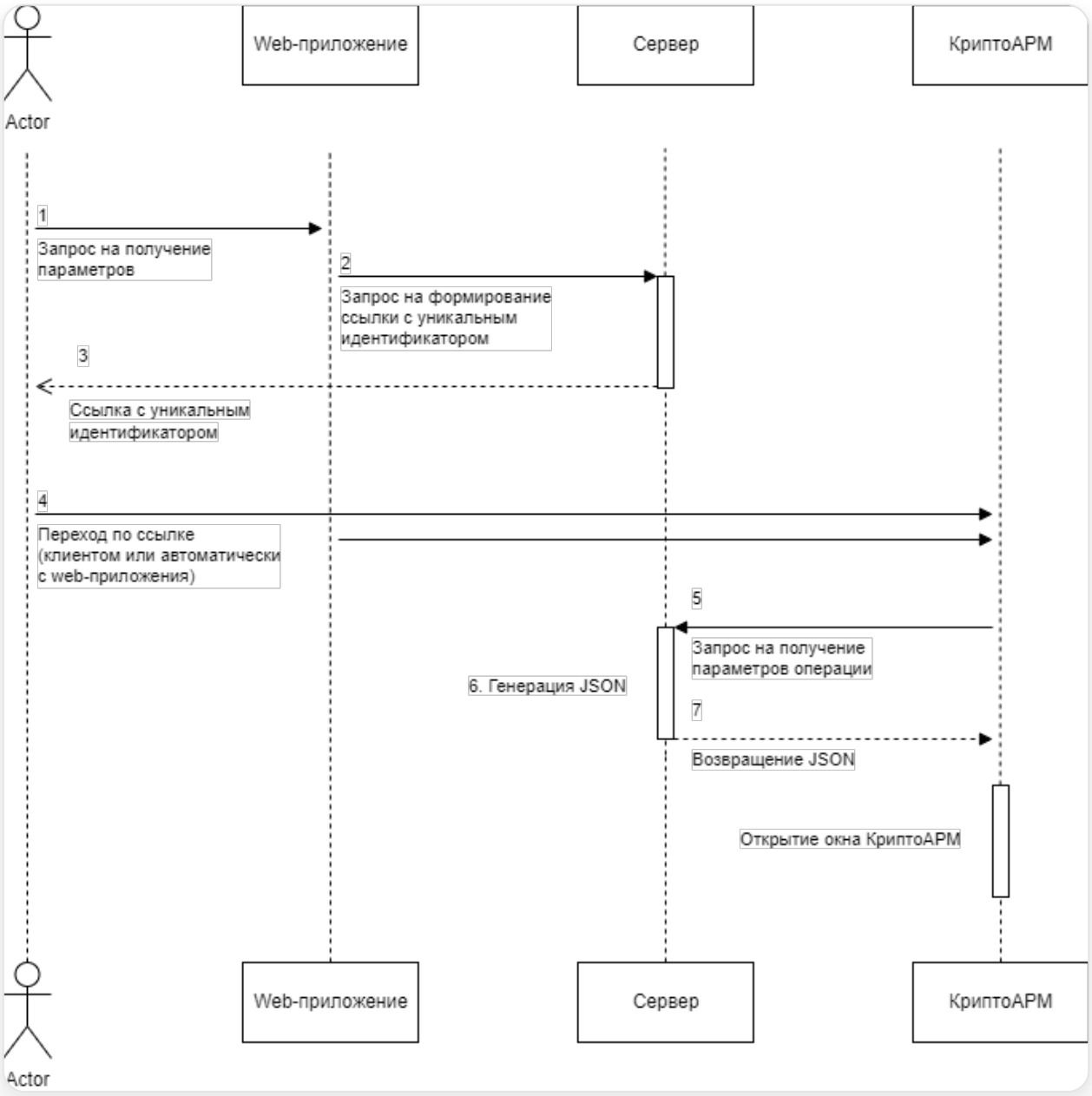
Команда startView

- Общая информация
- Формат ссылки
- Получение параметров операции
- Интерфейс IStartViewParameters
- Интерфейс IStartViewOperationProps

Общая информация

Команда `startView` используется для открытия конкретного окна приложения КриптоАРМ.

Схема взаимодействия:



Все запросы между КриптоАРМ и сервером ДОЛЖНЫ соответствовать спецификации протокола JSON-RPC 2.0.

В качестве транспорта используется HTTP.

> 🔍 Общее описание указано в разделе Формат ссылки.

Формат ссылки

Для выполнения команды `startView` должна быть сформирована ссылка вида:

```
cryptoarm://startView/<URL>/?id=<id>
```

- `cryptoarm://` - зарегистрированный протокол
- `startView` - выполняемая команда
- `<URL>` - ссылка на получение JSON с параметрами, нужными для выполнения команды
- `id` - уникальный идентификатор транзакции

Пример:

```
cryptoarm://startView/https://example.com/json?id=2c48eb32-a0a8-405c-ade9-eed130605cba
```

Получение параметров операции

После получения команды `startView` КриптоАРМ отправляет запрос на получение параметров операции.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`startView.parameters`	Используемый метод. Всегда `startView.parameters`.
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию. 🔍 Формат ссылки
diagnostic	`IDiagnosticInformaton`	Диагностическая информация о рабочем месте

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "startView.parameters",
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
    "diagnostic": {
    }
}
```

Формат ответа

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
result	`IStartViewParameters`	Объект со сведениями о параметрах операции
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию. 🔍 Формат ссылки

Пример:

```
HTTP/1.1 200 OK
Connection: close
Content-Length: ...
Content-Type: application/json
Date: Sat, 08 Jul 2020 12:04:08 GMT
{
    "jsonrpc": "2.0",
    "result": {
        " uiView": “CERTIFICATES_MY”,
        "props": {
            "headerText": "ИС cryptoarm.ru",
            "descriptionText": "Запрос на открытие окна"
        }
    },
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Интерфейс IStartViewParameters

Объекты данного типа описывают вид операции и её параметры.

Ключ	Значение	Описание
uiView	string	Тип окна, которое нужно отобразить пользователю. Доступные значения: - “MAIL” – окно почты, - “DOCUMENTS” – окно Документы, - “SIGN_AND_ENCRYPT” - окно подписи и шифрования, - “CERTIFICATES_MY” - окно Сертификаты/Личные

Ключ	Значение	Описание
		сертификаты, - “CERTIFICATES_ADDRESS_BOOK” - окно Сертификаты/Другие пользователи, - “CERTIFICATES_CA” - окно Сертификаты/Промежуточные, - “CERTIFICATES_ROOT” - окно Сертификаты/Корневые, - “CONTACTS” - окно Контакты, - “KEYS” - окно Сертификаты/ Список контейнеров, - “ABOUT” и “DIAGNOSTIC” - окно О программе (Настройки).
props	`IStartViewOperationProps`	Параметры операции

Интерфейс IStartViewOperationProps

Интерфейс `IStartViewOperationProps` описывает параметры операции.

Свойство	Тип	Описание
headerText?	string	Необязательный параметр. Используется для отображения в заголовке окна. Максимальная длина - 40 символов.
descriptionText?	string	Необязательный параметр. Используется для отображения в сведениях об операции. Максимальная длина - 120 символов.

Открыть статью на сайте

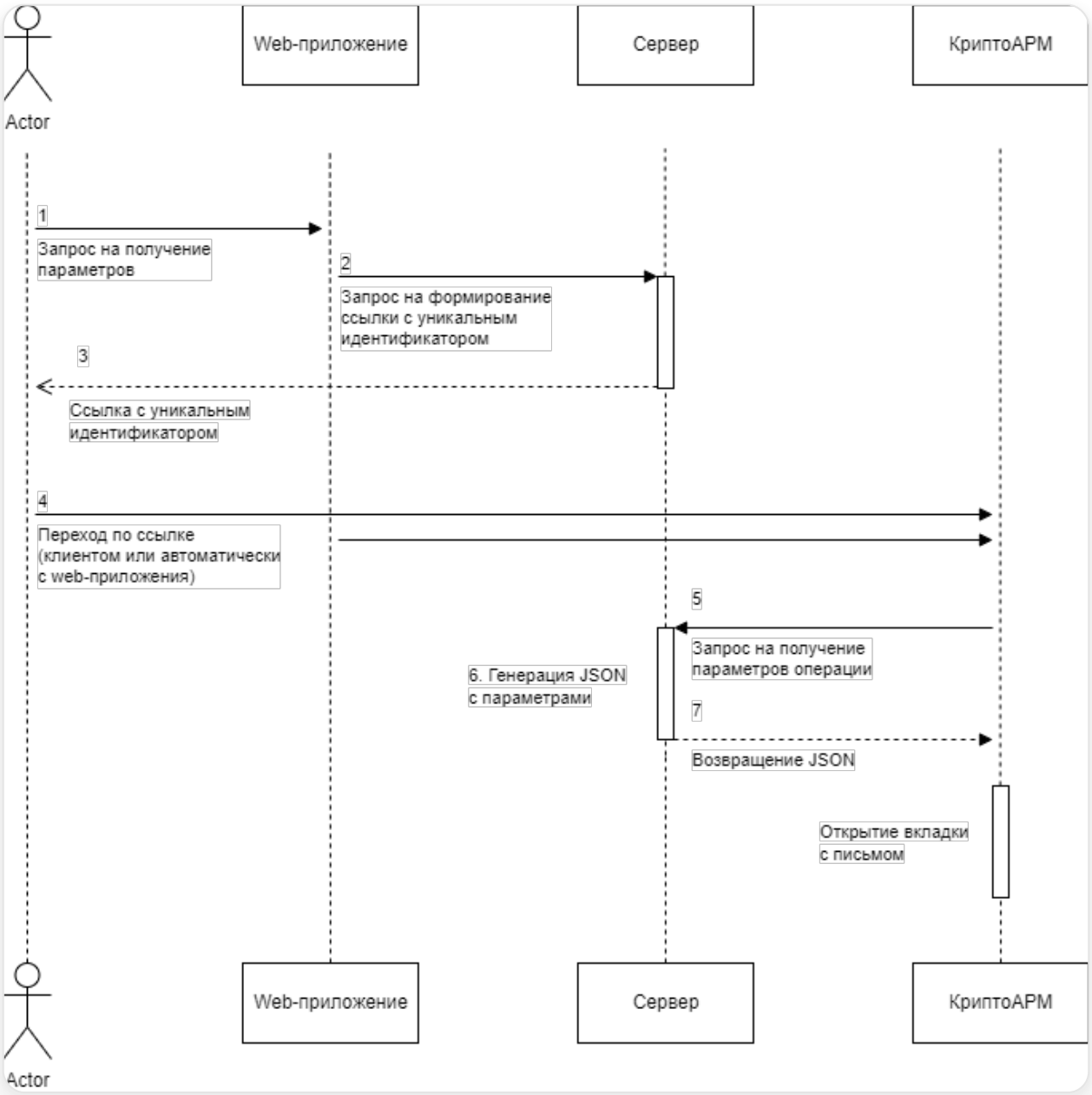
Команда mail

- Общая информация
- Формат ссылки
- Получение параметров операции
- Интерфейс IMailParameters
- Интерфейс IMailOperationProps
- Интерфейс IMailProps

Общая информация

Команда `mail` используется для действий с электронными письмами в КриптоАРМ.

Схема взаимодействия:



Все запросы между КриптоАРМ и сервером ДОЛЖНЫ соответствовать спецификации протокола JSON-RPC 2.0.

В качестве транспорта используется HTTP.

> 🔍 Общее описание указано в разделе Формат ссылки.

Формат ссылки

Для выполнения команды `mail` должна быть сформирована ссылка вида:

```
cryptoarm://mail/<URL>/?id=<id>
```

- `cryptoarm://` - зарегистрированный протокол
- `mail` - выполняемая команда
- `<URL>` - ссылка, на которую КриптоАРМ будет слать запросы
- `id` - уникальный идентификатор транзакции

Пример:

```
cryptoarm://mail/https://example.com/json?id=2c48eb32-a0a8-405c-ade9-eed130605cba
```

Получение параметров операции

После получения команды `mail` КриптоАРМ отправляет запрос на получение параметров операции.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`mail.parameters`	Используемый метод. Всегда `mail.parameters`.
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию. 🔍 Формат ссылки
diagnostic	`IDiagnosticInformaton`	Диагностическая информация о рабочем месте

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "mail.parameters",
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
    "diagnostic": {
    }
}
```

Формат ответа

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
result	`IMailParameters`	Объект со сведениями о параметрах операции
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию. 🔍 Формат ссылки

Пример ответа:

```
HTTP/1.1 200 OK
Connection: close
Content-Length: ...
Content-Type: application/json
Date: Sat, 08 Jul 2020 12:04:08 GMT
{
    "jsonrpc": "2.0",
    "result": {
        "operation": "SEND",
        "props": {
        "mailProps": {
           "to": ["test@example.com"],
           "cc": ["test1@example.com", "test2@example.com"],
           "bcc": ["test3@example.com"],
           "subject": "Message subject",
           "content": "text message content",
           "htmlContent": "<div>HTML message content</div>",
           "attachments": [{
                    "name": "file1.txt",
                    "url": "http://localhost:8080/public/files/file1.txt",
                    "id": 1,
                    "urlDetached": ""
                },
                {
                    "name": "file2.txt",
                    "url": "http://localhost:8080/public/files/file2.txt",
                    "id": 2,
                    "urlDetached": ""
                },
                {
                    "name": "file4.pdf",
                    "url": "http://localhost:8080/public/files/file4.pdf",
                    "id": 4,
                    "urlDetached": ""
                }
           ],
           "sign": false,
           "encrypt": false,
           "deliveryReport": false,
```

```
            "readReport": false
            }
        }
    },
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Интерфейс IMailParameters

Объекты данного типа описывают вид операции и её параметры.

Свойство	Тип	Описание
operation	string	Тип операции. Доступные значения: - «SEND» – открыть новое сообщение (черновик) с переданными параметрами, - «OPEN» – открыть для чтения сообщение eml.
props	`IMailOperationProps`	Параметры операции

Интерфейс IMailOperationProps

Объекты данного типа описывают вид операции и её параметры.

Свойство	Тип	Описание
eml?	`IFile`	Необязательный параметр. Параметры для получения eml файла.
mailProps?	`IMailProps`	Необязательный параметр. Свойства для нового сообщения.
extra?	Объект типа `IExtra`	Необязательный параметр. Настройки операции. Для команды `mail` это свойство может содержать `token`, для скачивания eml с сервера.

Интерфейс IMailProps

Объекты данного типа описывают параметры операции электронного сообщения.

Свойство	Тип	Описание
to	string[]	Массив адресов получателей
cc?	string[]	Массив адресов получателей копии
bcc?	string[]	Массив адресов получателей скрытой копии
subject	string	Тема сообщения
content	string	Текстовое содержимое сообщения
htmlContent?	string	Форматированное содержимое сообщения в формате HTML
attachments?	`IFile[]`	Файлы для прикрепления к сообщению (вложения)
sign	boolean	Флаг, указывающий на необходимость подписать сообщение
encrypt	boolean	Флаг, указывающий на необходимость зашифровать сообщение
deliveryReport	boolean	Флаг, включающий получение отчета о доставке
readReport	boolean	Флаг, включающий получение отчета о прочтении